

Département Informatique  
Economie, Gestion, Organisation et Droit  
DROIT DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

## TD N°1 DROIT DE L'INTERNET ET ENCADREMENT DES DONNEES A CARACTERE PERSONNEL

### 1. INFORMATIQUE ET LIBERTES : QUE FERIEZ VOUS ?

Annexe 1+ Amphi 2

Vous êtes responsable d'un supermarché qui a subi ces derniers mois de nombreux vols à la fois dans le magasin mais aussi dans les stocks. Vous souhaitez mettre en place un système de vidéosurveillance mais vous devez de respecter la législation en vigueur à savoir la Loi Informatique et Liberté en conformité avec le Règlement Général de Protection des Données entré en vigueur au mois de Mai 2018..

- 1.Elaborez une « mini » analyse d'impact relative à la protection dite PIA (Privacy Impact Assessment) en répondant au formulaire en annexe 1.
2. Rédigez une information à l'attention des personnes concernées par le dispositif de surveillance.
3. Un employé qui a été désigné comme délégué syndical souhaite consulter les enregistrements. Le peut-il ?

## 2. LES ACTIVITES PROSELYTES DES TEMOINS DE JHOVAHS ET LA PROTECTION DES DONNES PERSONNELLES

Annexe 2

1. Faites un résumé des faits en indiquant les parties et les juridictions saisies dans un premier temps.
2. Pourquoi la Cour de Justice de l'Union Européenne est-elle saisie ?
3. Formulez les questions juridiques auxquelles la CJUE va devoir répondre ?
5. Le constat de la Cour signifie t-il que les communautés religieuses ne peuvent pas collecter des données à caractère personnel dans le cadre d'une activité de prédication de porte-à-porte ?

1) La communauté des témoins de Jéhovah ont une activité de prédication en porte à porte. Ils en profitent pour récupérer des informations sur les habitants (nom, prénom, adresse, religion). La CNIL locale a interdit de récupérer ces données (manque de finalité). Le Tribunal a invalidé l'interdiction. Le défendeur des droits de la filippine.

2) Car il y a difficulté pour la juridiction nationale d'appliquer les réglementations européennes.

3) L'activité de prédication (en porte à porte) produit-elle des données personnelle ? (activité privée / professionnelle ?)

4) Non. Le soucis c'est pas que ça se fait dans une com. religieuse mais le non respect des conditions légales de collecte.

ANNEXE 1 PIA simplifié

S'agit-il de donnée à caractère personnel ?	Elles permettent d'identifier une personne de manière individuelle donc il s'agit de données à caractère personnel.
S'agit-il de donnée sensible ?	L'image d'une personne peut donner lieu à discrimination, il s'agit donc d'une donnée sensible.
S'agit-il d'un traitement de données ?	Il y aura un traitement par un employé (+ enregistrement et conservation)
Quelle peut être la finalité ?	Dissuader et identifier les auteurs des vols pour mener des poursuites judiciaires.
Est-elle pertinente et proportionnelle ?	Oui car son usage se limite à la surveillance des locaux. → intérêt légitime
Combien de temps seront conservées les images ?	Elles peuvent être conservées jusqu'à un mois
Qui sera responsable du traitement ?	Le responsable de la sécurité du magasin
Quelle(s) mesure(s) de sécurité peuvent être prises ?	<del>Il n'y a pas de mesures de sécurité.</del>
Où peuvent se situer les caméras de surveillance ?	zone de circulation et zone marchande (pas de surveillance des postes de travail et employé)
Est ce qu'il faut faire une déclaration auprès de la Cnil ?	Non mais le dispositif doit être autorisé par le préfet.
Comment faire respecter les droits des personnes ?	Informez du dispositif par un affichage conforme informant le visiteur de ses droits.

Tietosuojavaltuutettu / Uskonnollinen yhdyskunta

1/ La demande de décision préjudicielle porte sur l'interprétation de l'article 2, ainsi que de l'article 3 de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données .

2/Cette demande a été présentée dans le cadre d'une procédure engagée par le tietosuojavaltuutettu (contrôleur de la protection des données, Finlande) au sujet de la légalité d'une décision de la tietosuojalautakunta (commission de protection des données, Finlande) interdisant à la Jehovan todistajat – uskonnollinen yhdyskunta (communauté religieuse des témoins de Jéhovah, ci-après la « communauté des témoins de Jéhovah ») de collecter ou de traiter des données à caractère personnel dans le cadre de l'activité de prédication de porte-à-porte sans que les conditions de la législation finlandaise relative au traitement des données à caractère personnel soient respectées.

3 /Les considérants 10, 12, 15, 26 de la directive 95/46 énoncent :

« (10) considérant que l'objet des législations nationales relatives au traitement des données à caractère personnel est d'assurer le respect des droits et libertés fondamentaux, notamment du droit à la vie privée reconnu également dans l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et dans les principes généraux du droit communautaire ; que, pour cette raison, le rapprochement de ces législations ne doit pas conduire à affaiblir la protection qu'elles assurent mais doit, au contraire, avoir pour objectif de garantir un niveau élevé de protection dans la Communauté ;

(12) considérant que les principes de la protection doivent s'appliquer à tout traitement de données à caractère personnel dès lors que les activités du responsable du traitement relèvent du champ d'application du droit communautaire ; que doit être exclu le traitement de données effectué par une personne physique dans l'exercice d'activités exclusivement personnelles ou domestiques, telles la correspondance et la tenue de répertoires d'adresses ; aussi bien au traitement automatisé qu'au traitement manuel

(15) considérant que les traitements portant sur de telles données ne sont couverts par la présente directive que s'ils sont automatisés ou si les données sur lesquelles ils portent sont contenues ou sont destinées à être contenues dans un fichier structuré selon des critères spécifiques relatifs aux personnes, afin de permettre un accès aisé aux données à caractère personnel en cause ;

(26) considérant que les principes de la protection doivent s'appliquer à toute information concernant une personne identifiée ou identifiable ;

4/ L'article 1er, paragraphe 1, de la directive 95/46 dispose :

« Les États membres assurent, conformément à la présente directive, la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel. »

5/ L'article 2 de cette directive prévoit :

« Aux fins de la présente directive, on entend par :

a) "données à caractère personnel" : toute information concernant une personne physique identifiée ou identifiable (personne concernée) ; est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale ;

b) "traitement de données à caractère personnel" (traitement) : toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction ;

c) "fichier de données à caractère personnel" (fichier) : tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique ;

d) "responsable du traitement" : la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel ; lorsque les finalités et les moyens du traitement sont déterminés par des dispositions législatives ou réglementaires nationales ou communautaires, le responsable du traitement ou les critères spécifiques pour le désigner peuvent être fixés par le droit national ou communautaire ;

[...]

Le litige au principal :

- **Le 17 septembre 2013**, la commission de protection des données a adopté, à la demande du contrôleur de la protection des données, une décision interdisant à la communauté des témoins de Jéhovah de collecter ou de traiter des données à caractère personnel dans le cadre de l'activité de prédication de porte-à-porte effectuée par ses membres sans que les conditions légales du traitement de telles données, soient respectées. En outre, la commission de protection des

données a imposé à cette communauté, de faire en sorte que, dans un délai de six mois, aucune donnée à caractère personnel ne soit collectée pour les finalités de cette communauté sans que lesdites conditions soient respectées.

- Dans les motifs de sa décision, la commission de protection des données a considéré que la collecte des données en cause par les membres de la communauté des témoins de Jéhovah constituait un traitement de données à caractère personnel, au sens de ladite loi, et que cette communauté ainsi que ses membres étaient, conjointement, les responsables de ce traitement.

- La communauté des témoins de Jéhovah a saisi le Helsingin hallinto-oikeus (tribunal administratif de Helsinki, Finlande) d'un recours contre cette décision. Par jugement du 18 décembre 2014, cette juridiction a annulé ladite décision au motif, notamment, que la communauté des témoins de Jéhovah n'était pas responsable du traitement de données à caractère personnel, au sens de la loi finlandaise, et que l'activité de celle-ci ne constituait pas un traitement illégal de telles données.

- Le contrôleur de la protection des données a contesté ce jugement devant le Korkein hallinto-oikeus (Cour administrative suprême, Finlande).

- Selon les constatations de cette juridiction, les membres de la communauté des témoins de Jéhovah prennent, dans le cadre de leur activité de prédication de porte-à-porte, des notes sur les visites rendues à des personnes qu'eux-mêmes ou ladite communauté ne connaissent pas. Les données collectées pourraient, entre autres, comporter le nom et l'adresse des personnes démarchées ainsi que des informations portant sur leurs convictions religieuses et leur situation familiale. Ces données seraient collectées à titre d'aide-mémoire, et afin de pouvoir être retrouvées pour une éventuelle visite ultérieure, sans que les personnes concernées y aient consenti ni n'en aient été informées.

-Toujours selon les constatations de la juridiction de renvoi, la communauté des témoins de Jéhovah a donné à ses membres des lignes directrices relatives à la prise de telles notes, lignes directrices figurant au moins dans une de ses revues consacrées à l'activité de prédication. Cette communauté et les paroisses qui en dépendent organiseraient et coordonneraient l'activité de prédication de porte-à-porte de leurs membres, notamment en établissant des cartes à partir desquelles des secteurs seraient répartis entre les membres assurant l'activité de prédication et en tenant des fiches sur les prédicateurs et le nombre de publications de la communauté diffusées par ceux-ci. En outre, les paroisses de la communauté des témoins de Jéhovah gèreraient une liste des personnes ayant exprimé le souhait de ne plus faire l'objet de visites de la part des membres prédicateurs, et les données à caractère personnel figurant sur cette liste, dite « liste d'interdiction », seraient utilisées par les membres de cette communauté. Enfin, la communauté des témoins de Jéhovah aurait, dans le passé, tenu à la disposition de ses membres des formulaires aux fins de la collecte desdites données au cours de leur activité de prédication. L'utilisation de ces formulaires aurait, toutefois, été abandonnée à la suite d'une recommandation du contrôleur de la protection des données.

- La juridiction de renvoi fait observer que, selon les propres indications de la communauté des témoins de Jéhovah, celle-ci n'exige pas de ses membres prédicateurs qu'ils procèdent à une collecte de données et que, dans les cas où une telle collecte a tout de même lieu, elle n'a connaissance ni de la nature des notes prises, lesquelles ne sont au demeurant que des notes personnelles informelles, ni de l'identité des membres prédicateurs ayant procédé à la collecte.

- S'agissant de la nécessité de la présente demande de décision préjudicielle, le Korkein hallinto-oikeus (Cour administrative suprême) considère que l'examen de l'affaire au principal exige de tenir compte, d'une part, des droits à la protection de la vie privée et à la protection des données personnelles et, d'autre part, de la liberté de religion et d'association, garantis tant par la Charte et la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales que par la constitution finlandaise.

- La juridiction de renvoi tend à considérer que l'activité de prédication de porte-à-porte pratiquée par les membres d'une communauté religieuse, telle que la communauté des témoins de Jéhovah, ne relève pas des activités exclues du champ d'application de la directive 95/46 en vertu de son article 3, paragraphe 2, premier tiret.

- En revanche, la question se pose de savoir si cette activité présente un caractère exclusivement personnel ou domestique. À cet égard, il conviendrait de tenir compte du fait que, en l'occurrence, les données collectées vont au-delà de simples notes figurant dans un carnet d'adresses, puisque les notes prises se rapportent à des inconnus et contiennent des données sensibles relatives à leurs convictions religieuses. Devrait également être pris en considération le fait que l'activité de prédication de porte-à-porte est une forme d'action essentielle de la communauté des témoins de Jéhovah, organisée et coordonnée par cette dernière et par ses paroisses.

- Par ailleurs, dans la mesure où les données collectées en cause au principal sont traitées de manière non automatisée, il y aurait lieu, de déterminer si l'ensemble de ces données constitue un fichier, au sens de ces dispositions. Selon les informations fournies par la communauté des témoins de Jéhovah, lesdites données ne lui sont pas communiquées, si bien qu'il n'est pas possible de connaître avec certitude la nature et l'ampleur des données collectées. Cependant, il serait possible de considérer que le but de la collecte et du traitement ultérieur des données en cause au principal est de pouvoir retrouver aisément les données concernant une personne ou une adresse déterminée aux fins d'une utilisation ultérieure. Les données collectées ne seraient néanmoins pas structurées sous forme de fiches.

- Dans le cas où le traitement des données en cause au principal relèverait du champ d'application de la directive 95/46, la juridiction de renvoi souligne que la question se poserait alors de savoir si la communauté des témoins de Jéhovah doit être considérée comme étant responsable de ce traitement. La jurisprudence de la Cour issue de l'arrêt du 13 mai 2014, Google Spain et Google (C-131/12, EU:C:2014:317), définirait de manière large la notion de « responsable du traitement ». En outre, il convient de prendre en compte, notamment, le pouvoir de contrôle effectif et la conception que la personne dont les données sont traitées se fait du responsable du traitement.

Département Informatique

Economie, Gestion, Organisation et Droit

DROIT DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

## TD N°2.1 L'ENCADREMENT DU COMMERCE ELECTRONIQUE

### 1. « DO NOT TRACK »

Annexes 1&2 + <https://donottrack-doc.com/fr/about/>

"Do not track » est une série documentaire interactive sur le tracking et l'économie du web, en ligne depuis le 14 avril 2015 qui a reçu le Peabody Award 2016, décerné par l'Université de Géorgie, à Athens (Etats-Unis).

1. Rappelez l'élément central du RGPD.
2. Quels sont les reproches formulés par l'association « la quadrature du net » à l'encontre de GAFAM ?
3. Expliquez le paragraphe suivant « Le Conseil norvégien des consommateurs travaille avec d'autres organisations, comme l'UFC-Que choisir en France, pour faire pression et hisser ces mauvaises pratiques à l'agenda politique. Quant à savoir si elles sont illégales et répréhensibles, Finn Myrstad s'en remet aux organismes de régulation: «*Nous avons envoyé des lettres aux autorités compétentes*». »
4. Comment définiriez vous « l'éthique » ? Faites vous une distinction entre éthique et légalité.
5. A partir du lien hypertexte et de votre propre expérience, complétez la grille d'analyse en annexe 2 puis élaborer par groupe (deux ou trois max) une carte mentale ou dite heuristique (avec ou sans logiciel) sur le thème « Les traces que je laisse sur Internet ».

## **2. TWITTER DOIT-IL SE FAIRE APPLIQUER LE DROIT DE LA CONSOMMATION ?**

Annexe 3

1. Dites quelles sont les parties et la juridiction saisie ainsi que le motif de la saisine.
  2. Expliquez à quelle condition une clause est reconnue comme étant abusive et la conséquence de cette qualification.
  3. Les dispositions du droit de la consommation doivent-elles s'appliquer à Twitter selon la justice ? Pourquoi ?
  4. Quels sont les principaux griefs formulés à l'encontre de Twitter ?
  5. Quelle solution apporte la justice dans sa décision ?
-

### 3. LE GEO BLOCAGE SUR INTERNET (POUR ALLEZ PLUS LOIN)

Annexe 4

1. De quoi dépend en règle générale la fixation d'un prix ?
2. Les prix sont-ils libres ?
3. Qu'est ce que l'indice Big Mac ?
4. Expliquez le concept de prix géo localisé.
5. Expliquez le cas Disneyland.
6. Que disent les articles 18 et 20 du traité de fonctionnement de l'Union Européenne ?
7. Qu'est ce que le yield management ?
8. Quelles seront prochainement les nouvelles règles ?

## ANNEXE 1 RGPD: Google, Facebook et Microsoft utilisent le webdesign pour tromper l'internaute

slate.fr

July 24, 2018 04:01 AM

Vous souvenez-vous du flot d'e-mails qui a inondé vos messageries il y a quelques semaines? «La protection des données personnelles est un enjeu important», nous assurait chaque expéditeur avant de nous inviter à consulter sa «nouvelle politique de confidentialité» comme un homme politique clamant qu'il «a changé». Pourtant, ces changements n'ont rien à voir avec leur bonne volonté mais avec le Règlement européen sur la protection des données (RGPD), effectif depuis le 25 mai dernier.

Voté en 2016, ce texte contraint entreprises, associations et organismes publics à obtenir le consentement explicite des internautes avant de réclamer leurs données personnelles... en théorie. Mais certains semblent ne pas s'y résigner. Comme les Gafam (Google, Amazon, Facebook, Apple et Microsoft), tout aussi accro à nos données que nous à leurs services.

### Le webdesign au service du capitalisme

Les géants du web utilisent des «pièges» pour bernier les utilisateurs et utilisatrices et les amener à livrer le maximum de données les concernant. Ces «dark patterns» –terme inventé par le webdesigner anglais Harry Brignull en 2010– sont des astuces pensées dans l'interface d'un site internet pour «capturer l'utilisateur et faire en sorte qu'il y reste», définit le webdesigner français Geoffrey Dorne. Parmi les catégories de dark patterns identifiées par Harry Brignull, on trouve le «Privacy Zuckering», ou «Zuckerage de la vie privée»: «Lorsque vous êtes poussé à partager toujours plus d'informations sur vous-même que vous ne l'aviez prévu». Si typique sur Facebook que Harry Brignull lui a donné un sobriquet qui rappelle le créateur du réseau social numéro un.

Heureusement, les choses ont changé depuis l'arrivée du RGPD. Les premiers à se targuer de respecter la nouvelle législation étaient les Gafam. Vraiment? Ce ne sont pas les conclusions du rapport «Deceived by design», réalisé entre avril et juin 2018 par le réactif Conseil norvégien des consommateurs sur les pratiques de Facebook, Google et Windows 10.

### Gafam et données personnelles: incitation ou manipulation?

«Nous voulions regarder le processus du consentement, commence Finn Myrstad, directeur des services numériques de l'organisation. Les trois services utilisent des techniques pour encadrer l'information.» C'est-à-dire des astuces peu éthiques. Le Conseil reproche aux trois services de diriger l'utilisateur de manière insidieuse là où ils veulent l'emmener. Par exemple, Google culpabilise la personne qui refuserait d'activer la géolocalisation arguant que ce service permet de lui proposer des suggestions plus appropriées, donc plus ciblées. En général, il n'en faut pas plus pour se plier à la volonté du géant.

Pire, le Conseil norvégien des consommateurs dénonce des mensonges par omission sur la publicité ciblée. Facebook présente ainsi la reconnaissance faciale comme un outil «qui aide les malvoyants et protège des utilisateurs malveillants» sans ajouter qu'elle lui sert à cibler encore plus les publicités affichées.

Geoffrey Dorne va d'ailleurs plus loin: pour lui, toutes ces technologies de reconnaissance –faciale ou digitale– relèvent de la vie privée et ne devraient pas servir à s'authentifier: «Si je me fais pirater un mot de passe, je le change, j'en invente ou j'en génère un nouveau. Par contre, le jour où je me fais pirater la reconnaissance de mon visage ou mon empreinte digitale, je ne pourrai pas la changer».

Selon le rapport, Windows 10 semble plus respectueux du consentement des utilisateurs et utilisatrices que les deux autres firmes. Néanmoins, Microsoft fait bien sentir, par les mots utilisés, que la publicité ci-

«Cela est une chose positive et que s'en passer serait dommage car «le nombre de pubs que vous verrez ne changera pas, mais celles-ci pourraient être moins pertinentes pour vous». Un tel langage vous déçoit-il? Normal, c'est le but.

Formulaire de mise en conformité au RGPD	Facebook	Google	Microsoft
Absence de paramètres intrusif par défaut	X	X	OK
Facilité d'accès aux options respectant la vie privée	X	X	OK
Le design ne pousse pas à choisir des options intrusive pour la vie privée	X	X	X
Les intitulés ne poussent pas à choisir des options intrusives pour la vie privée	X	X	X
Les options respectant la vie privée ne sont pas accompagnées d'avertissements	X	X	OK
Les utilisateurs peuvent repousser leur décision d'accepter de livrer leurs données tout en accédant au service	X	X	X

Conclusions du rapport «Design by deceived». | Réalisation tableau: Kevin Poireault

Ces exemples, et bien d'autres encore, vont à l'encontre de l'obligation de consentement libre et explicite caractérisé par le RGPD. Pire, pour ceux et celles qui ne veulent pas accepter de se livrer un peu, Facebook propose une seule option: supprimer son compte. Cette alternative extrême est interdite si l'on en croit le RGPD.

**«Nous espérons que les Gafam changeront leurs méthodes manipulatrices, pas du tout éthiques»,** souffle Finn Myrstad. Le Conseil norvégien des consommateurs travaille avec d'autres organisations, comme l'UFC-Que choisir en France, pour faire pression et hisser ces mauvaises pratiques à l'agenda politique. Quant à savoir si elles sont illégales et répréhensibles, Finn Myrstad s'en remet aux organismes de régulation: «Nous avons envoyé des lettres aux autorités compétentes».

### «C'est un problème de modèle économique»

En France, la Commission nationale de l'informatique et des libertés (Cnil) a partagé la lettre «avec les autres autorités européennes» mais admet qu'il «n'y a pas de réponse apportée pour le moment». Finn Myrstad nous a également transmis la réponse de Google et de Facebook, qui lui proposent d'en discuter au retour de vacances. Une réunion en vidéoconférence entre le Conseil norvégien et les multinationales est prévue pour début septembre.

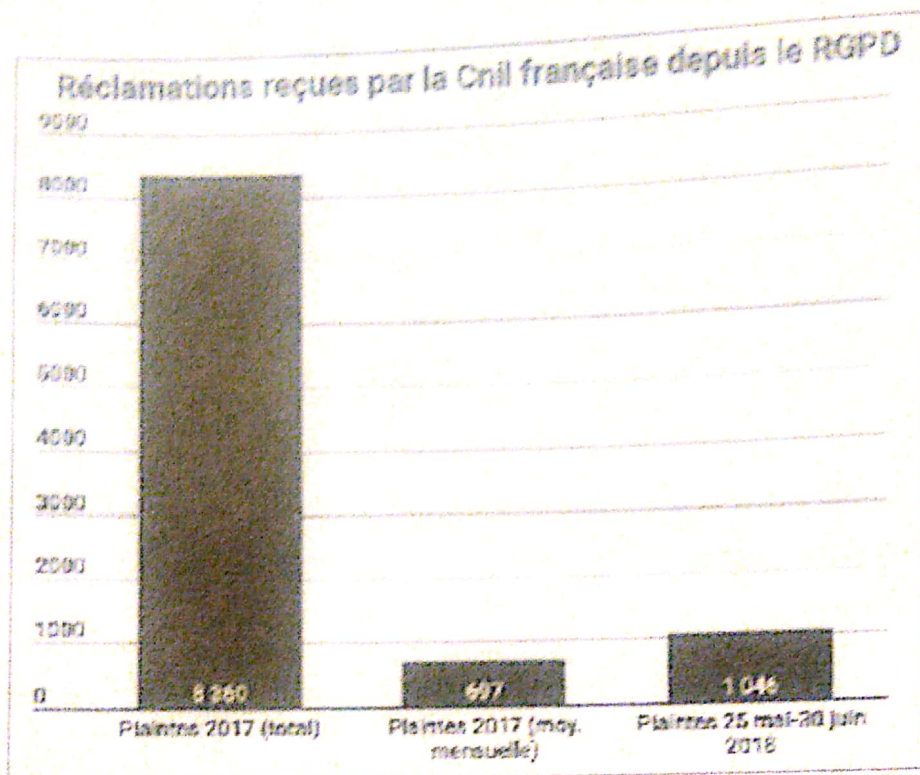
«C'est jouer à leur jeu que de tirer de telles conclusions, rétorque Arthur Messaud, juriste à la Quadrature du Net, association luttant pour la protection des données. Le problème n'est pas dans le design ou le langage utilisé. C'est un problème de modèle économique. Ces acteurs pensent qu'on peut acheter des libertés fondamentales. En utilisant leurs services, le consentement ne sera jamais valide.»

Geoffrey Dorne acquiesce: «Le modèle économique des sites internet est encore majoritairement basé sur la publicité ciblée. Ils ont donc besoin de beaucoup d'audience pour gagner de l'argent». D'où le besoin de capturer l'utilisateur ou utilisatrice. Coûte que coûte.

### Plus de 1.000 plaintes en un mois

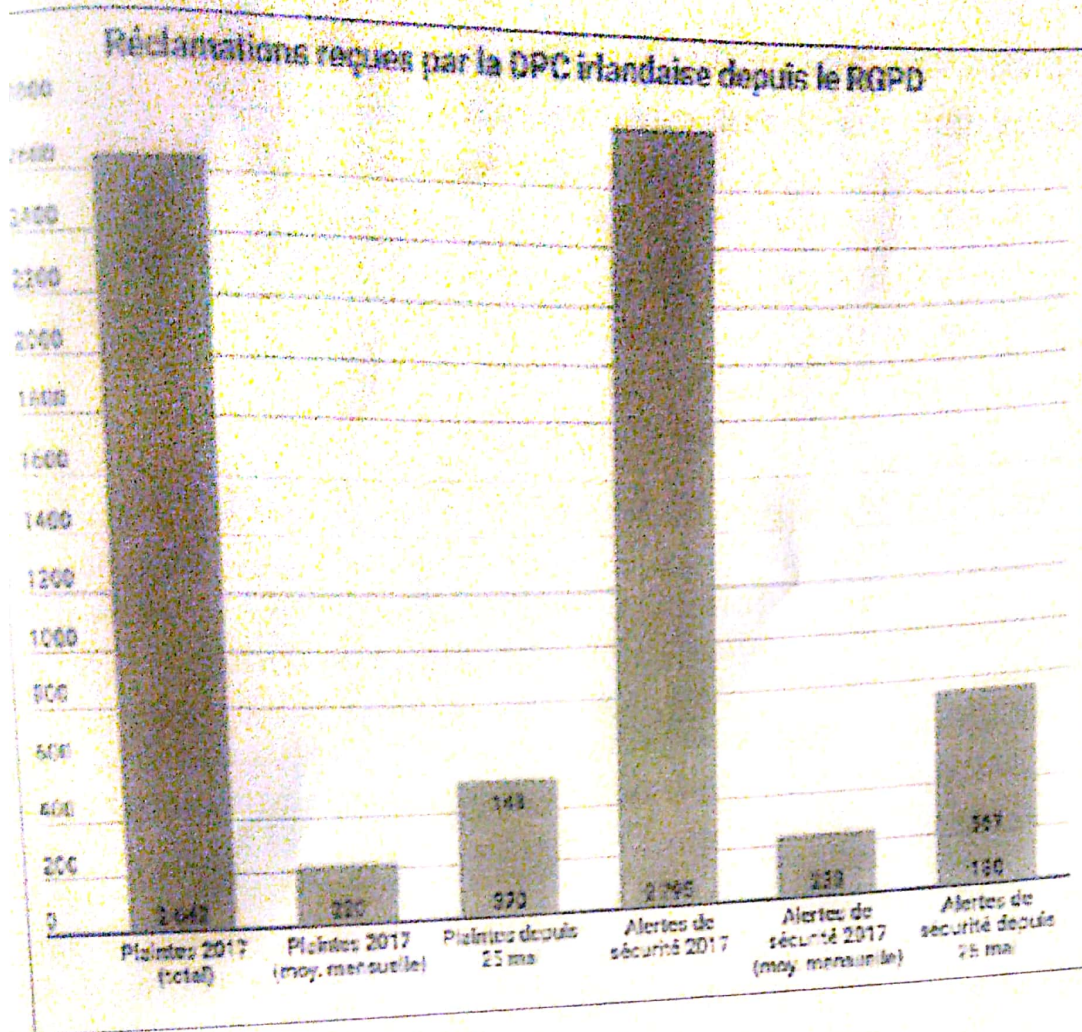
Arthur Messaud, lui, veut se battre sur le terrain de la loi. Les plaintes en tout genre auprès de la Cnil ont bondi: l'organisme a reçu 1.046 réclamations entre le 25 mai et le 30 juin, contre une moyenne mensuelle d'à peine 700 en 2017. Une augmentation de 43%.

Réalisation infographie: Kevin Poireault



Trois jours seulement après l'arrivée du RGPD, la Quadrature du Net a envoyé à la Cnil cinq plaintes collectives contre Google, Amazon, Facebook, Apple et LinkedIn. «Ces entreprises pouvaient déjà être poursuivies, souligne le juriste. Mais nous avons attendu le RGPD pour faire en sorte que les débats soient très concrets, avec une vraie base légale. Nous avons aussi besoin du texte pour mener des plaintes collectives.» Cet arsenal juridique a en effet été créé par la nouvelle législation européenne. L'association française est soutenue par 12.000 internautes dans ces actions en justice déposées auprès de la Cnil, qui a promis un retour d'ici un mois –que la Quadrature attend toujours.

Si ces plaintes sont recevables, la Cnil les confiera aux autorités des pays européens dans lesquels les Gafam sont installés: la Data Protection Commission en Irlande pour Google, Facebook et Apple et la Commission nationale luxembourgeoise pour la protection de données pour Amazon. Le siège de Microsoft Europe, lui, est basé en France. L'organisme concerné mènera alors son enquête. Une fois fixé, le chef européen des Cnil, le Comité européen de la protection des données, prendra une décision, avec un vote à la majorité s'il y a un désaccord. «Nous sommes les tout premiers à leur envoyer des plaintes collectives, précise Arthur Messaud. Avec nous, ils essuient les plâtres.»



Réalisation infographie: Kevin Poireault

### Après le greenwashing, le privacy-washing

Contactée par téléphone, l'entreprise Amazon France assure qu'elle a toujours respecté la loi et qu'elle est conforme au RGPD. Microsoft et Google nous ont promis une réponse, pour l'instant sans résultat. Facebook et Apple n'ont pas encore répondu malgré de multiples relances. Sans attendre un processus qui peut «prendre entre un et deux ans» selon Arthur Messaud, la Quadrature compte envoyer quatre autres plaintes collectives à la Cnil. Cette fois-ci, les services visés sont Whatsapp, Instagram, Android, et deux services de Microsoft, Outlook et Skype. «Comme il y a du greenwashing, on a aujourd'hui du privacy-washing, où le respect de la vie privée devient un argument commercial, analyse Geoffrey Dorne. Ce n'est pas toujours vrai, c'est même parfois malhonnête.»

Récemment, Google a écopé d'une amende de 4,3 milliards d'euros par l'Europe pour abus de position dominante. Or, la firme de Mountain View serait susceptible de payer une somme similaire avec la plainte de la Quadrature, affirme l'association. Un autre activiste du net, l'Autrichien Maximilian Schrems, évalué à 7,6 milliards d'euros l'ensemble des sanctions si ses quatre plaintes (contre Android, Instagram, Whatsapp et Facebook) sont jugées en sa faveur. En attendant, la prochaine fois qu'on vous assure respecter vos données, veuillez bien à vérifier les cases précochées avant d'y croire.

## ANNEXE 3 L'adhésion à Twitter est un contrat de consommation LEGALIS MARDI 04 SEPTEMBRE 2018

Dans une décision fleuve de 235 pages, le TGI de Paris a déclaré illicites 265 des clauses actuelles ou anciennes des « Conditions d'utilisation », de la « Politique de confidentialité » et des « Règles de Twitter » sur les 269 épinglées par l'association UFC Que Choisir, à l'origine de l'action en justice. Twitter ne s'est pas encore prononcé sur sa décision d'interjeter appel, mais il est probable qu'il le fasse.

Intervenu le 7 août 2018, en pleines vacances estivales, le jugement n'a peut-être pas eu toute la publicité qu'il mérite. Premier point remarquable de la décision, le TGI a affirmé que « le contrat d'utilisation de la plate-forme, exploitée par la société Twitter en sa qualité de professionnel, est soumis aux dispositions du code de la consommation, notamment aux dispositions relatives aux clauses abusives, l'utilisateur qui participe au contenu restant un consommateur au regard des dispositions du code de la consommation. ». Twitter avait invoqué le caractère gratuit de son offre de service pour exclure l'application du droit de la consommation. Le tribunal commence par rappeler que, selon le code civil, le contrat à titre onéreux est celui par lequel les parties reçoivent un avantage en contrepartie de celui qu'elle procure. Or, si Twitter propose des services sans contrepartie monétaire, elle commercialise à titre onéreux les données personnelles ou non de ses utilisateurs déposées gratuitement lors de leur inscription au site ou de son utilisation. Il s'agit donc bien d'un contrat à titre onéreux, au sens de l'article 1107 du code civil. « En conséquence, en collectant des données déposées gratuitement par l'utilisateur à l'occasion de son accès à la plate-forme et en les commercialisant à titre onéreux, la société Twitter, agissant à des fins commerciales, tire profit de son activité, de sorte qu'il est un « professionnel » au sens de l'article liminaire du code de la consommation, lequel définit le professionnel, comme toute personne physique ou morale, publique ou privée, agissant à des fins entrant dans le cadre de son activité commerciale, y compris lorsqu'elle agit au nom ou pour le compte d'un autre professionnel. », a conclu le tribunal qui en a déduit que Twitter est soumis au droit de la consommation, notamment aux dispositions relatives aux clauses abusives.

Autre point important du jugement, le tribunal a considéré que Twitter est le responsable du traitement de données personnelles. C'est lui qui détermine les finalités du site et qui doit, en conséquence, prendre les précautions utiles pour assurer la sécurité des données. Contrairement à ce que prétend le réseau social, l'utilisateur ne peut donc pas être responsable des conséquences qui découleraient d'une utilisation de son compte, même par un tiers non autorisé. Le tribunal a donc jugé que la loi Informatique et libertés est opposable à Twitter Inc. et Irl., quand bien même elles ne sont pas installées sur le territoire français.

Le tribunal a notamment jugé illicites les clauses qui prévoient que les données personnelles sont « publiques » par défaut, qui autorisent le transfert des données personnelles dans un autre pays sans autres précisions, à copier, adapter, modifier, vendre les contenus postés ou futurs des utilisateurs, y compris ceux protégés par le droit de la propriété intellectuelle, à tout bénéficiaire sur tout support, sans autorisation préalable, à clôturer le compte d'un utilisateur en conservant notamment son nom sans limitation de durée, etc.

## ANNEXE 4 Peut-on "géolocaliser" le prix dans le commerce électronique ?

[droit-technologie.org/actualites/peut-on-geolocaliser-le-prix-dans-le-commerce-electronique](http://droit-technologie.org/actualites/peut-on-geolocaliser-le-prix-dans-le-commerce-electronique)

01/06/2015

Publié le 31/05/2015 par Etienne Wery

La plupart des gens l'ignorent, mais lorsqu'on achète en ligne, il arrive souvent que le prix affiché varie en fonction de l'endroit où se trouve l'acheteur. Pour la même robe, une Française ou une Belge ne payeront pas le même prix. C'est le « prix géo localisé ».

### Le commerce traditionnel

Au départ, il y a une évidence : le prix de vente d'un bien dépend de son prix de revient, et le prix de revient dépend lui-même de facteurs locaux.

La fabrication d'une robe, effectuée dans une usine centralisée, revient un prix déterminé. Disons 10 €.

Cette robe sera ensuite envoyée dans l'ensemble des pays dans lesquels la marque dispose de magasins, et le prix de vente au public pourra varier. C'est logique : une boutique sur les Champs-Élysées coûte plus cher qu'une boutique à Bruxelles, le salaire de la vendeuse belge coûte plus cher que celui de sa collègue polonaise, l'envoi de la robe en Grèce coûte plus cher que l'envoi à Berlin jusque à côté de l'usine, etc.

C'est cela qui explique que dans le commerce traditionnel, le prix d'un même bien peut varier. La robe qui revenait à 10 € en sortie d'usine, sera vendue 15 € à Berlin, 17 € à Bruxelles et 20 € à Paris.

Personne n'a jamais remis cela en cause, dans la mesure où cette différenciation se fonde sur des motifs objectifs et non-discriminatoires.

Ce qui précède est tellement vrai, que certains (d'abord par amusement mais très sérieusement ensuite), étudient ces variations. L'indice Big Mac en est une application : bien que la recette du Big Mac soit rigoureusement identique dans le monde entier, son prix de vente final peut varier du simple au double (voire plus) et les économistes en tirent des enseignements par rapport au PIB, au pouvoir d'achat et à l'indice de bien-être des pays concernés.

### Le modèle de tarification Club Med

Le mythique opérateur de village de vacances est un modèle du genre en matière de prix géolocalisé.

La même semaine dans un village de vacances revient à 2.000 € pour un belge, et à 3.000 € pour un français. La semaine suivante, ce sera l'inverse : le français payera 1.000 € de moins que le belge. Que le belge n'essaye pas d'acheter via une boutique française, car il sera renvoyé vers son réseau national, et vice-versa.

Certes, il y a dans le prix une partie qui couvre les frais de transport, et ceux-ci peuvent varier en fonction du point de départ du client.

Mais après avoir couvert le transport, il reste une différence très importante alors qu'on peut raisonnablement penser que sur place, le Belge et le Français coûtent environ la même chose au Club Med.

Hors transport, le Club fait donc payer plus ou moins cher en fonction de lieu de résidence et/ou du passeport de son client.

Il y a différentes raisons qui sont avancées par cela, notamment au niveau du coût du réseau dans chacun des pays, mais la réalité est que l'essentiel de la variation du prix dépend des vacances, et l'on sait que les périodes de vacances ne sont pas les mêmes dans les pays européens.

Certaines voix se sont élevées, mais personne n'a trouvé la parade infaillible.

### L'arrivée de l'Internet

Les choses évoluent avec la généralisation du commerce en ligne.

Il y a quelques années, sur l'Internet, le prix géolocalisé était un phénomène relativement rare. L'Internet était au contraire vécu comme un espace unique et son corollaire, le prix unique, récoltait un large consensus, d'autant que le réseau était de plus en plus occupé par des marques pan-européennes.

Petit à petit, les choses ont changé et le prix géolocalisé a fait son grand retour.

Il y a deux semaines, à l'occasion du vote du nouveau paquet numérique au Parlement européen, un député s'est livré en séance un exercice très instructif. Il a réservé en ligne auprès de Disneyland Paris, en prenant soin de s'identifier de pays européens différents. Les conclusions sont tranchantes : le député a observé des prix pouvant varier de 865 à 1.272 € pour la même prestation. Le député a renouvelé l'expérience pour divers services et a à chaque fois constaté la même chose. Ainsi, sur Zalando, la même robe coûte plus cher à Paris qu'à Bruxelles.

Le problème est tellement complexe que le vice-président de la Commission européenne s'en est emparé. Il est en effet difficile de plaider la création d'un marché unique de l'internet en Europe, si l'on observe en même temps des différences de prix aussi importantes pour lesquelles on peine à déceler une différenciation fondée sur une base objective et non discriminatoire.

On observe dans la foulée le grand retour de l'article 20 du Traité sur le fonctionnement de l'Union européenne, instituant la citoyenneté européenne. Lu en combinaison avec l'article 18 (principe de non-discrimination sur la base de la nationalité) du TFUE, l'article 20 est traditionnellement interprété par la CJUE comme prohibant toute forme de discrimination sur la base de la nationalité.

Dès lors, raisonnant par analogie, plusieurs voix affirment aujourd'hui que la différenciation tarifaire fondée uniquement sur le lieu de résidence ou la nationalité de l'acheteur, est condamnable. Ces voix partent du postulat selon lequel les dispositions invoquées sont applicables horizontalement (c'est-à-dire entre personnes physiques et/ou morales, par opposition à l'applicabilité verticale qui ne fait guère de doute).

### **Ne pas confondre avec le yield management**

On le voit, le prix géolocalisé est au centre de toutes les attentions des autorités européennes.

Il ne faut toutefois pas confondre cette problématique avec celle du yield management.

Le yield management est un système de gestion dans lequel le prix varie en temps réel en fonction de la demande. Ce modèle de gestion est issu du monde de l'hôtellerie et du transport aérien, où l'on sait que le prix du billet d'avion pour une même destination peut changer du tout au tout d'un jour à l'autre, parce que la date de départ approche et que l'avion se remplit (ou pas).

Dans le yield management, ce n'est pas la géolocalisation qui modifie le prix mais la disponibilité du produit ou du service (bref, le rapport entre l'offre et la demande), ce qui pose moins de souci juridique.

### **L'Europe interdit le géo-blocage sur Internet**

Vous êtes belge et réservez un séjour dans un hôtel en France. Votre belle-famille, italienne, réserve la même chambre au même moment mais paye moins cher. Vous êtes français et achetez un ordinateur en ligne sur un site allemand, et êtes redirigé vers le site français 20% plus cher. C'est l'effet de la géo-localisation des prix. Dans un an, ce sera fini !

Le Parlement européen, le Conseil et la Commission ont conclu un accord politique mettant fin aux blocages géographiques injustifiés pour les consommateurs désirant acheter des produits ou des services en ligne dans l'Union.

Objectif des nouvelles règles : dynamiser le commerce électronique en faveur des consommateurs et des entreprises qui tireront parti de la croissance du marché en ligne européen.

Pour les citoyens, cela signifie qu'ils pourront acheter leurs appareils électriques en ligne, louer une voiture ou acheter des places de concert à l'étranger comme ils le font dans leur propre pays. Ils ne seront plus confrontés à des obstacles tels que la contrainte de payer avec une carte de débit ou de crédit émise dans un autre pays que le leur. Pour les entreprises, cela signifie une plus grande sécurité juridique pour exercer des activités à l'étranger.

Pas de géo-blocage dans les cas suivants ...

Les nouvelles règles définissent trois situations spécifiques dans lesquelles il n'existe ni justification ni critères objectifs permettant de concevoir un traitement différent a priori entre les clients de différents États membres.

- La vente de biens sans livraison physique. Exemple: Un consommateur belge souhaite acheter un réfrigérateur et trouve la meilleure offre sur un site web allemand. Il pourra commander le produit et le retirer dans les locaux du négociant ou organiser lui-même la livraison à son domicile. S'il y a une différence de prix, ce ne peut donc être que pour des raisons liées à la livraison, dont le coût varie fortement en fonction de l'éloignement des parties.
- La vente de services fournis par voie électronique. Exemple: Vous préférez faire héberger votre site web en Espagne plutôt qu'en Belgique : vous aurez désormais accès au service, et vous pourrez vous enregistrer et acheter ce service sans avoir à payer de frais supplémentaires par rapport à un consommateur espagnol.
- La vente de services fournis dans un lieu physique précis. Exemple: Une famille italienne peut acheter directement un voyage vers un parc d'attractions en France sans être redirigée vers un site internet italien. Elle paiera le même prix qu'une famille française (on se souvient que Disneyland Paris avait été épinglé comme un des exemples de géo-blocage inopportun).

## TD N°3 LA RESPONSABILITE SUR LE WEB

### 1. CAS PRATIQUE : IMAGE ET VIDEO

#### Annexe 1

Alexandre, 17 ans : « Lors d'une journée au lycée, j'ai fait le pari que je pourrais filmer un cours de français avec mon téléphone. J'ai réussi à en filmer une partie et le moment où la prof s'énervait était si drôle que mes amis m'ont demandé de leur envoyer la vidéo. L'un deux l'a mise en ligne sur youtube et Facebook.

Les commentaires qui ont suivi étaient tous assez virulents et le nombre de visionnages augmentait. J'ai voulu supprimer la vidéo mais elle n'était plus sous mon contrôle. »

Une plainte a été déposée avec constitution de partie civile.

1. Citez les acteurs et qualifiez les juridiquement.
2. Déterminez leur niveau de responsabilité.
3. Identifiez les sanctions encourus pour chacun d'entre eux.

## ANNEXE 1 EXTRAITS D'ARTICLES DE LOI ET DE JURISPRUDENCE

L'article 9 du Code civil énonce que « chacun a droit au respect de sa vie privée », y compris au respect de son image. Le juge rappelle souvent que « toute personne a sur son image un droit exclusif et absolu et peut s'opposer à sa fixation, à sa reproduction ou à son utilisation sans autorisation préalable ».

Par ailleurs, le **Code pénal** prévoit des sanctions spécifiques en la matière :

- le fait de photographier ou filmer une personne sans son consentement, se trouvant dans un lieu privé ou de transmettre l'image ou la vidéo, est puni d'un an d'emprisonnement et de 45 000 euros d'amende.
- le fait de capter, conserver, diffuser ou laisser diffuser l'image d'une personne prise dans un lieu privé sans le consentement de celle-ci, est puni d'un an d'emprisonnement et de 45 000 euros d'amende ;
- le fait de publier le montage réalisé avec l'image d'une personne sans son consentement est puni d'un an d'emprisonnement et de 15 000 euros d'amende.

### La loi pour la confiance dans l'économie numérique définit les régimes juridiques applicables sur Internet :

- l'auteur est le créateur du contenu qui peut être une œuvre originale ou non (un texte, une vidéo, une photo, un article posté sur un blog, etc.) ; dans le cas d'un blog ou de pages personnelles, il en est également l'éditeur ;
- l'éditeur d'un contenu : qu'il soit ou non à l'origine du contenu, il en assure au moins la maîtrise éditoriale ;
- le fournisseur d'un service de communication en ligne est celui qui crée un service (forum, blog, etc.). Il peut proposer un espace de rédaction à des auteurs ;
- l'hébergeur est la structure qui fournit les moyens techniques pour donner accès à des sites internet. Il assure le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature ;
- le fournisseur d'accès à Internet (ou FAI) offre un service donnant la possibilité d'accéder au réseau internet.

Les conséquences juridiques de ces qualifications sont importantes, car l'auteur d'un contenu, l'éditeur, l'hébergeur et le FAI ont des obligations et des responsabilités différentes en cas de contenu litigieux.

Extrait Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique -

#### Article 6

Face à un contenu illégal (racisme, injure, atteinte à la vie privée, contrefaçon...) publié sur internet (texte, vidéo, photo, commentaire...), la victime peut déposer plainte contre l'auteur. L'hébergeur sera responsable uniquement s'il a délibérément mis en ligne ou laissé en ligne ce contenu illicite.

#### Jurisprudence sur la responsabilité de l'hébergeur, affaire INA / YouTube

- o Le Tribunal, statuant en audience publique, par jugement contradictoire, en premier ressort,
  - Dit que l'action de l'INA est recevable.
  - Dit que la société Youtube doit se voir appliquer le régime de responsabilité réservé aux hébergeurs par la loi du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN).
  - Dit que la diffusion et le maintien par la société Youtube d'extraits de programmes audiovisuels appartenant au catalogue de l'INA, sans l'autorisation de ce dernier, **après que leur illicéité ait été signalée, et le fait qu'elle n'ait pas empêché la remise en ligne de ces programmes**, constitue la contrefaçon prévue par les articles L 122-4 et L 215-1 du Code de la propriété intellectuelle.

Département Informatique  
Economie, Gestion, Organisation et Droit  
DROIT DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

TD N°4 LA PROTECTION DES OEUVRES NUMERIQUES

**1. LA QUESTION DELICATE DES LIENS HYPERTEXTES**

**Annexe 1**

1. Présentez brièvement les faits.
2. Dites pour quelle raison la Bundesgerichtshof (Cour fédérale de justice allemande) a saisi la CJUE ?
3. Expliquez ce que recouvre la notion de « communication au public » ?
4. Rappelez les prérogatives attachées au droit d'auteur dont il est question ici.
5. Distinguez la mise en ligne de la mise à disposition au moyen d'un lien cliquable renvoyant au site sur lequel la communication initiale a été effectuée.
6. Exposez la position de la CJUE.

## **2. CONDITIONS DE PROTECTION DES LOGICIELS PAR LE DROIT D'AUTEUR**

### Annexe 2

1. Identifiez les parties et la juridiction saisie.
  2. Résumez les faits à l'origine de la saisine.
  3. Précisez le fondement de la demande d'Anaphore.
  4. Relevez au regard de quel critère la juridiction examine le litige.
  5. Dites quelle a été la décision et surtout ses motivations.
-

## ANNEXE 1 ARRÊT DE LA COUR (deuxième chambre) 7 août 2018

Dans l'affaire C-161/17, ayant pour objet une demande de décision préjudicielle au titre de l'article 267 TFUE, introduite par le Bundesgerichtshof (Cour fédérale de justice, Allemagne), par décision du 23 février 2017, parvenue à la Cour le 31 mars 2017, dans la procédure Land Nordrhein-Westfalen contre Dirk Renckhoff,

La demande de décision préjudicielle porte sur l'interprétation de l'article 3, paragraphe 1, de la directive 2001/29/CE du Parlement européen et du Conseil, du 22 mai 2001, sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information (JO 2001, L 167, p. 10).

Cette demande a été présentée dans le cadre d'un litige opposant le Land Nordrhein-Westfalen (Land de Rhénanie-du-Nord-Westphalie, Allemagne) à M. Dirk Renckhoff, photographe, au sujet de l'utilisation sans autorisation, par une élève d'une école se situant dans le ressort dudit Land, d'une photographie réalisée par M. Renckhoff et librement disponible sur un site Internet, aux fins d'illustrer un exposé scolaire publié par cette école sur un autre site Internet.

Le cadre juridique :

Il convient de maintenir un juste équilibre en matière de droits et d'intérêts entre les différentes catégories de titulaires de droits ainsi qu'entre celles-ci et les utilisateurs d'objets protégés. [...] »

L'article 3 de la directive 2001/29, intitulé « Droit de communication d'œuvres au public et droit de mettre à la disposition du public d'autres objets protégés », dispose, à ses paragraphes 1 et 3 : « 1. Les États membres prévoient pour les auteurs le droit exclusif d'autoriser ou d'interdire toute communication au public de leurs œuvres, par fil ou sans fil, y compris la mise à la disposition du public de leurs œuvres de manière que chacun puisse y avoir accès de l'endroit et au moment qu'il choisit individuellement. [...] 3. Les droits visés aux paragraphes 1 et 2 ne sont pas épuisés par un acte de communication au public, ou de mise à la disposition du public, au sens du présent article. »

L'article 5 de la directive 2001/29, intitulé « Exceptions et limitations », dispose, à son paragraphe 3, sous a) : « Les États membres ont la faculté de prévoir des exceptions ou limitations aux droits prévus aux articles 2 et 3 dans les cas suivants : a) lorsqu'il s'agit d'une utilisation à des fins exclusives d'illustration dans le cadre de l'enseignement ou de la recherche scientifique, sous réserve d'indiquer, à moins que cela ne s'avère impossible, la source, y compris le nom de l'auteur, dans la mesure justifiée par le but non commercial poursuivi ».

Le litige au principal et la question préjudicielle

M. Renckhoff, partie requérante ayant saisi le Landgericht Hamburg (tribunal régional de Hambourg, Allemagne), est photographe. La Stadt Waltrop (ville de Waltrop, Allemagne), qui était initialement partie défenderesse en première instance, mais qui n'est plus partie au litige au

principal, a sous sa responsabilité la Gesamtschule de Waltrop (établissement d'enseignement secondaire de Waltrop, ci-après l'« école »). Le Land de Rhénanie-du-Nord-Westphalie (Allemagne), également partie défenderesse en première instance, est chargé du contrôle de l'école et est l'employeur des enseignants de cette dernière.

À compter du 25 mars 2009, il était possible de consulter sur le site Internet de l'école un exposé rédigé par l'une de ses élèves dans le cadre d'un atelier linguistique proposé par celle-ci, lequel comportait, à titre d'illustration, une photographie réalisée par M. Renckhoff (ci-après la « photographie »), que cette élève avait téléchargée sur un site Internet consacré aux voyages (ci-après le « site Internet de voyage »). La photographie se trouvait sur ce dernier site sans mesure de restriction empêchant son téléchargement. Sous celle-ci, l'élève avait indiqué une référence audit site.

M. Renckhoff fait valoir qu'il n'a donné un droit d'utilisation qu'aux exploitants du site Internet de voyage et prétend que la mise en ligne de la photographie sur le site Internet de l'école porte atteinte à son droit d'auteur. Il a demandé à la juridiction compétente en première instance qu'il soit interdit au Land de Rhénanie-du-Nord-Westphalie, sous peine d'astreinte, de reproduire ou de permettre la reproduction et/ou de mettre à la disposition ou de permettre la mise à la disposition du public de la photographie et, à titre subsidiaire, de permettre aux élèves de reproduire la photographie afin de la mettre sur Internet. Il a également réclamé le paiement, par ledit Land, d'une somme de 400 euros à titre de dommages et intérêts.

Le recours de M. Renckhoff ayant été partiellement accueilli, le Land de Rhénanie-du-Nord-Westphalie a été condamné à retirer la photographie du site Internet de l'école et à payer une somme de 300 euros, majorée des intérêts.

Les deux parties ont fait appel de ce jugement devant l'Oberlandesgericht Hamburg (tribunal régional supérieur de Hambourg, Allemagne), qui a considéré, notamment, que la photographie était protégée par le droit d'auteur et que sa mise en ligne sur le site Internet de l'école avait porté atteinte aux droits de reproduction et de mise à la disposition du public, dont M. Renckhoff est titulaire. Cette juridiction a estimé que la circonstance que la photographie était déjà accessible à tous sans restriction sur Internet, avant les agissements litigieux, était dénuée de pertinence, la reproduction de la photographie sur le serveur et la mise à la disposition du public qui s'est ensuivie sur le site Internet de l'école ayant entraîné un « découplage » avec la publication initiale sur le site Internet de voyage.

Saisie d'un pourvoi en Revision, la juridiction de renvoi considère que l'issue de ce pourvoi dépend de l'interprétation de l'article 3, paragraphe 1, de la directive 2001/29. En particulier, cette juridiction éprouve des doutes quant à la satisfaction de l'exigence, consacrée par la jurisprudence, selon laquelle la communication au public concerné doit avoir été faite à un public « nouveau ».

Dans ces conditions, le Bundesgerichtshof (Cour fédérale de justice, Allemagne) a décidé de surseoir à statuer et de poser à la Cour la question préjudicielle suivante :

« l'insertion, sur un site Internet accessible au public, d'une œuvre libéralement diffusée sur l'ensemble des internautes sur un autre site Internet avec l'autorisation du titulaire du droit d'auteur consentus et elle une mise à la disposition du public, au sens de l'article 3, paragraphe 1, de la directive 2001/29, lorsque l'œuvre a d'abord été copée sur un serveur puis, de là, téléchargée sur le site Internet ? »

sur la question préjudicielle

Par sa question, la juridiction de renvoi demande, en substance, si la notion de « communication au public », au sens de l'article 3, paragraphe 1, de la directive 2001/29, doit être interprétée en ce sens qu'elle couvre la mise en ligne sur un site Internet d'une photographie préalablement publiée, sans mesure de restriction et avec l'autorisation du titulaire du droit d'auteur, sur un autre site Internet.

À titre liminaire, il y a lieu de rappeler qu'une photographie est susceptible d'être protégée par le droit d'auteur, à condition, ce qu'il appartient à la juridiction nationale de vérifier dans chaque cas d'espèce, qu'elle soit une création intellectuelle de l'auteur reflétant la personnalité de ce dernier et se manifestant par les choix libres et créatifs de celui-ci lors de la réalisation de cette photographie.

S'agissant de la question de savoir si la mise en ligne sur un site Internet d'une photographie préalablement publiée, sans mesure de restriction et avec l'autorisation du titulaire du droit d'auteur, sur un autre site Internet constitue une « communication au public », au sens de l'article 3, paragraphe 1, de la directive 2001/29, il y a lieu de rappeler que cette disposition prévoit que les États membres attribuent aux auteurs le droit exclusif d'autoriser ou d'interdire la communication au public de leurs œuvres.

Il en découle que, sous réserve des exceptions et limitations prévues, de façon exhaustive, à l'article 5 de la directive 2001/29, toute utilisation d'une œuvre effectuée par un tiers, sans un tel consentement préalable, doit être regardée comme portant atteinte aux droits de l'auteur de cette œuvre.

L'article 3, paragraphe 1, de la directive 2001/29 ne précisant pas la notion de « communication au public », il y a lieu de déterminer le sens et la portée de cette notion, au regard des objectifs poursuivis par cette directive et au regard du contexte dans lequel la disposition interprétée s'insère. Le Land de Rhénanie-du-Nord-Westphalie a en effet valoir, en se fondant notamment sur l'arrêt du 13 février 2014, Svensson e.a. (C-466/12, EU:C:2014:76), qu'il n'y a pas lieu d'établir une distinction entre, d'une part, la communication d'une œuvre par la mise en ligne de celle-ci sur un site Internet et, d'autre part, la communication d'une telle œuvre par l'insertion, sur un site Internet, d'un hyperlien qui renvoie à un autre site Internet sur lequel cette œuvre a été initialement communiquée, sans mesure de restriction et avec l'autorisation du titulaire du droit d'auteur. Ainsi, dans des circonstances telles que celles en cause au principal, l'œuvre ne serait pas communiquée à un public nouveau.

En revanche, M. Renckhoff lors de l'audience, de même que la Commission, dans ses observations écrites, ont soutenu, en substance, que la jurisprudence visée au point précédent du

présent arrêt n'est pas applicable dans des circonstances telles que celles en cause au principal. En particulier, la communication d'une œuvre au moyen, non pas d'un hyperlien, mais d'une nouvelle mise en ligne de celle-ci sur un site Internet différent du site sur lequel cette œuvre a déjà été communiquée avec l'autorisation du titulaire du droit d'auteur devrait être qualifiée de « nouvelle communication au public », eu égard notamment à la circonstance que, à la suite de cette nouvelle mise à disposition, ledit titulaire n'est plus en mesure d'exercer son pouvoir de contrôle sur la communication initiale de ladite œuvre.

À cet égard, il convient de rappeler, en premier lieu, qu'il ressort d'une jurisprudence constante de la Cour que, sous réserve des exceptions et limitations prévues à l'article 5 de la directive 2001/29, tout acte de reproduction ou de communication au public d'une œuvre par un tiers requiert le consentement préalable de son auteur et que les auteurs disposent, en vertu de l'article 3, paragraphe 1, de la directive 2001/29, d'un droit de nature préventive leur permettant de s'interposer entre d'éventuels utilisateurs de leur œuvre et la communication au public que ces utilisateurs pourraient envisager d'effectuer, cela afin d'interdire celle-ci.

Or, un tel droit de nature préventive serait privé d'effet utile dans l'hypothèse où il devrait être considéré que la mise en ligne sur un site Internet d'une œuvre préalablement publiée sur un autre site Internet et avec l'autorisation du titulaire du droit d'auteur ne constitue pas une communication à un public nouveau. En effet, une telle mise en ligne, sur un site Internet autre que celui sur lequel a été effectuée la communication initiale, pourrait avoir pour effet de rendre impossible ou, à tout le moins, nettement plus difficile l'exercice par le titulaire de son droit, de nature préventive, d'exiger qu'il soit mis fin à la communication de celle-ci, le cas échéant, en retirant l'œuvre dudit site Internet sur lequel celle-ci a été communiquée avec son autorisation ou en révoquant l'autorisation précédemment accordée à un tiers.

Ainsi, il en résulterait que, même dans l'hypothèse où le titulaire du droit d'auteur déciderait de ne plus communiquer son œuvre sur le site Internet sur lequel celle-ci a été initialement communiquée avec son autorisation, cette œuvre demeurerait disponible sur le site Internet sur lequel la nouvelle mise en ligne a été effectuée. Or, la Cour a déjà souligné que l'auteur d'une œuvre doit pouvoir mettre fin à l'exercice, par un tiers, des droits d'exploitation sous forme numérique qu'il détient sur cette œuvre, et lui en interdire ce faisant toute utilisation future sous

Or, considérer que la mise en ligne sur un site Internet d'une œuvre préalablement communiquée sur un autre site Internet avec l'autorisation du titulaire du droit d'auteur ne constitue pas une mise à la disposition d'un public nouveau de cette œuvre reviendrait à consacrer une règle d'épuisement du droit de communication.

{...}

Compte tenu de ces éléments, il y a lieu de considérer, au regard de la jurisprudence, que la mise en ligne d'une œuvre protégée par le droit d'auteur sur un site Internet autre que celui sur lequel a été effectuée la communication initiale avec l'autorisation du titulaire du droit d'auteur doit, dans des circonstances telles que celles en cause au principal, être qualifiée de mise à la disposition d'un public nouveau d'une telle œuvre. En effet, dans de telles circonstances, le public qui a été pris en compte par le titulaire du droit d'auteur lorsqu'il a autorisé la communication de

son œuvre sur le site Internet sur lequel celle-ci a été initialement publiée est constitué des seuls utilisateurs dudit site, et non des utilisateurs du site Internet sur lequel l'œuvre a ultérieurement été mise en ligne sans l'autorisation dudit titulaire, ou des autres internautes.

A la différence des hyperliens qui, selon la jurisprudence de la Cour, contribuent notamment au bon fonctionnement d'Internet en permettant la diffusion d'informations dans ce réseau caractérisé par la disponibilité d'immenses quantités d'informations (arrêt du 8 septembre 2016, *GS Media*, C-160/15, EU:C:2016:644, point 45), la mise en ligne sur un site Internet sans l'autorisation du titulaire du droit d'auteur d'une œuvre préalablement communiquée sur un autre site Internet avec l'accord dudit titulaire ne contribue pas, dans la même mesure, à un tel objectif.

Dans ce contexte, le Land de Rhénanie-du-Nord-Westphalie expose qu'il convient, dans des circonstances telles que celles en cause au principal, de tenir compte, dans la mise en balance des intérêts en présence, du droit à l'éducation, énoncé à l'article 14 de la charte des droits fondamentaux. En particulier, l'action de l'élève concernée relèverait de l'exercice dudit droit, dès lors que la photographie a été placée, à des fins d'illustration, en première page de l'exposé préparé par celle-ci dans le cadre d'un atelier linguistique. Toutefois, à cet égard, il suffit de constater que les considérations exposées au point 35 du présent arrêt, relatives à la notion de « public nouveau », sont fondées non pas sur la nature éducative ou non de l'illustration, par l'élève, de son exposé scolaire, mais sur la circonstance que la mise en ligne de cette œuvre sur le site Internet de l'école a rendu celle-ci accessible à l'ensemble des visiteurs de ce site.

Au demeurant, il convient de rappeler que, s'agissant de la recherche d'un équilibre entre le droit à l'éducation et la protection du droit de propriété intellectuelle, le législateur de l'Union a prévu, à l'article 5, paragraphe 3, sous a), de la directive 2001/29, une faculté pour les États membres de prévoir des exceptions ou limitations aux droits prévus aux articles 2 et 3 de cette directive pour autant qu'il s'agit d'une utilisation à des fins d'illustration exclusive dans le cadre de l'enseignement ou de la recherche scientifique, dans la mesure justifiée par le but non commercial poursuivi.

Deuxièmement, ainsi qu'il a été rappelé au point 29 du présent arrêt, les droits garantis aux auteurs par l'article 3, paragraphe 1, de la directive 2001/29 sont de nature préventive. Or, s'agissant de l'acte de communication que constitue l'insertion, sur un site Internet, d'un hyperlien qui renvoie à une œuvre préalablement communiquée avec l'autorisation du titulaire du droit d'auteur, la nature préventive des droits du titulaire est préservée, dès lors qu'il est loisible à l'auteur, dans l'hypothèse où il ne souhaite plus communiquer son œuvre sur le site Internet concerné, de retirer celle-ci du site Internet sur lequel elle a initialement été communiquée, rendant caduc tout hyperlien renvoyant vers celle-ci. En revanche, dans des circonstances telles que celles en cause au principal, la mise en ligne sur un autre site Internet d'une œuvre engendre une nouvelle communication, indépendante de la communication initialement autorisée. En conséquence de cette mise en ligne, une telle œuvre serait susceptible de demeurer disponible sur ce dernier site, indépendamment du consentement préalable de l'auteur et en dépit de toute action par laquelle le titulaire de droits déciderait de ne plus communiquer son œuvre sur le site Internet sur lequel celle-ci a été initialement communiquée avec son autorisation.

En l'occurrence, il ressort de la décision de renvoi que l'utilisatrice de l'œuvre en cause au principal a fait une reproduction de cette œuvre sur un serveur privé, suivie d'une mise en ligne de celle-ci sur un site Internet autre que celui sur lequel a été réalisée la communication initiale. Ce faisant, cette utilisatrice a joué un rôle décisif dans la communication de cette œuvre à un public qui n'était pas pris en compte par l'auteur de celle-ci lorsqu'il a autorisé la communication initiale.

Eu égard à l'ensemble des considérations qui précèdent, il y a lieu de répondre à la question posée que la notion de « communication au public », au sens de l'article 3, paragraphe 1, de la directive 2001/29, doit être interprétée en ce sens qu'elle couvre la mise en ligne sur un site Internet d'une photographie préalablement publiée, sans mesure de restriction empêchant son téléchargement et avec l'autorisation du titulaire du droit d'auteur, sur un autre site Internet.

Par ces motifs, la Cour (deuxième chambre) dit pour droit :

La notion de « communication au public », au sens de l'article 3, paragraphe 1, de la directive 2001/29/CE du Parlement européen et du Conseil, du 22 mai 2001, sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information, doit être interprétée en ce sens qu'elle couvre la mise en ligne sur un site Internet d'une photographie préalablement publiée, sans mesure de restriction empêchant son téléchargement et avec l'autorisation du titulaire du droit d'auteur, sur un autre site Internet.

Le conseil général de l'Eure (désormais dénommé conseil départemental) a conclu, le 7 juillet 1997, une licence d'utilisation du logiciel Arkhéïa, développé par Anaphore pour l'accès et la gestion de ses fonds d'archives.

Ce contrat a ensuite donné lieu à plusieurs avenants.

Souhaitant se doter d'une nouvelle solution globale, destinée à promouvoir son patrimoine archivistique ainsi que le service des archives et à mettre à disposition de la recherche historique et citoyenne les instruments de recherche produits, le conseil départemental a lancé une procédure de marché public courant 2013.

Dans ce cadre, il a détaillé ses besoins et attentes dans un cahier des clauses techniques particulières daté du 4 juillet 2013.

Arkhéïa est par ailleurs un signe qui a été déposé et enregistré à l'INPI à titre de marque, en 1995.

La société Anaphore a alors écrit début août 2013 au conseil général de l'Eure lui reprochant d'avoir décrit, avec une extrême précision, l'architecture générale de son logiciel, la structure de ses données et de ses modes opératoires qu'elle estimait très spécifiques, et d'avoir renseigné, ainsi, tous ses concurrents commerciaux sur son savoir-faire, tout en citant à de multiples reprises son logiciel et présentant même des captures d'écran de ce dernier.

Le conseil général de l'Eure a répondu en octobre 2013 à ces allégations en faisant valoir que décrire les fonctionnalités d'un logiciel, même très précisément, ne pouvait constituer une atteinte aux droits de propriété intellectuelle de son éditeur.

La société Anaphore a alors fait appel en novembre 2013 à un expert informatique, inscrit près la cour d'appel de Nîmes, lequel a établi un rapport non contradictoire concluant à l'originalité du logiciel Arkhéïa.

Pour sa part, le conseil général avait retiré entre-temps son offre de marché public litigieuse avant de la réitérer dans des termes différents, en novembre 2013.

La société Naoned a finalement remporté, en janvier 2014, le marché public proposé.

Estimant que cette dernière société, de même que d'autres sociétés concurrentes, avaient développé de nouvelles solutions informatiques à partir des données relatives à son logiciel divulguées dans le cahier des charges du conseil général de l'Eure, la société Anaphore a fait assigner la collectivité territoriale devant le tribunal de grande instance de Lille en contrefaçon de son logiciel et de sa marque Arkhéïa.

Par jugement du 26 mai 2016, le tribunal de grande instance de Lille a :

– débouté la société Anaphore et M. X. de l'intégralité de leurs demandes ;

La société Anaphore a interjeté appel de cette décision, par déclaration reçue, par voie électronique, au greffe de la cour le 18 juillet 2016.

Dans le dernier état de leurs écritures récapitulatives, déposées par voie électronique le 18 janvier 2017, ils font appel du jugement et demandent à la cour de Constaté les actes de contrefaçon de logiciel et de marque du conseil départemental de l'Eure ;

Dire et juger que l'originalité du logiciel est présumée ;

Dire et juger qu'il appartient au conseil départemental de l'Eure de démontrer l'absence d'originalité ;

Constater que le conseil départemental de l'Eure n'apporte pas la preuve d'absence d'originalité.

En conséquence :

Condamner le conseil départemental de l'Eure à indemniser la société Anaphore et à lui verser à ce titre :

- 754.400 euros au titre de son préjudice commercial,
- 50.000 euros au titre de l'article 700 du code de procédure civile,
- 2.320 euros HT soit 2 779,36 euros au titre des frais et honoraires de l'expert Monsieur Sarton (Pièce n° 33),
- Aux entiers dépens ;

Dire et juger que les intérêts porteront eux-mêmes intérêts en application de l'article 1154 du code civil."

Aux termes de ses conclusions récapitulatives, déposées par voie électronique le 9 mars 2017, le conseil départemental de L'Eure demande à la cour de {...}

## DISCUSSION

\* Sur la demande en contrefaçon du droit d'auteur sur le logiciel Arkhéïa :

Que, pour être considéré comme original et bénéficier ainsi de la protection du droit d'auteur, un logiciel doit révéler un apport intellectuel propre et un effort personnalisé caractérisant les choix opérés par son concepteur, susceptible de l'affirmer comme une œuvre de l'esprit ;

Que l'effort personnalisé, de l'auteur d'un logiciel, doit aller au-delà de la simple mise en œuvre d'une logique automatique et contraignante, la matérialisation de cet effort résidant dans une structure individualisée ;

Qu'il appartient donc aux parties, qui invoquent la protection du droit d'auteur, de rapporter la preuve de ces éléments fondant le caractère original du logiciel ;

Attendu, en l'espèce, comme l'a relevé à bon droit le premier juge, que la société Anaphore et M. X. appuient essentiellement leur demande sur un "Rapport technique informatique", ni daté et ni signé, établi par M. Benoît Sarton, expert en informatique inscrit sur la liste des experts de la cour d'appel de Nîmes ;

Qu'ils persistent à se prévaloir des conclusions de ce rapport établi, à leur demande, de façon non contradictoire, par un expert qui n'a pas été judiciairement désigné ;

Attendu que M. Sarton fonde son argumentation sur un document intitulé "Cctp pour la ré-informatisation des archives départementales - Description du Logiciel Arkhéïa" daté du 3 février 2014, établi par la société Anaphore, postérieurement à l'appel d'offre litigieux de juillet 2013, pour les besoins de la cause soutenue par elle ;

Que si ce rapport revêt la valeur juridique d'une simple information, il ne suffit pas, en tout état de cause, à démontrer l'existence d'éléments originaux alors que son auteur s'est fondé exclusivement sur les déclarations de M. X., qu'il ne précise pas avoir examiné directement la solution informatique, qu'il procède par voie d'affirmation et qu'il ne fournit aucune démonstration effective de l'apport créatif de la société Anaphore et M. X. ;

Qu'il évoque une organisation de modules fonctionnels et une architecture de la base de données visant à répondre à des contraintes induites par la spécificité d'un service de gestions d'archives, tout en admettant d'emblée qu'il existe, en matière de création de logiciels d'informatisation des services d'archives, des outils informatiques "tout faits" ;  
Qu'ainsi, alors que le secteur des archives, contraint et codifié, ne laisse que peu de place au choix et au libre arbitre de l'auteur du logiciel – de sorte que la créativité s'en trouve forcément bridée -, la société Anaphore et M. X. énoncent, dans leurs propres écritures, que "Le créateur du logiciel Arkhéia a entièrement refondu son travail en 1997 afin que celui-ci soit conforme aux exigences apportées par la circulaire 97-4" ce qui apparaît exclusif de toute originalité propre à une œuvre de l'esprit protégeable ;

Attendu, enfin, que le moyen tiré de la reproduction illicite de la documentation préparatoire alléguée en cause d'appel manque en fait ;

Qu'en effet, le cahier des charges a été rédigé par le conseil départemental de l'Eure et non par la société Anaphore et il ne constitue nullement la reproduction d'une architecture originale en ce qu'il est issu de l'expérience du conseil départemental, sur la base de laquelle il a exprimé ses besoins ;

Qu'ainsi l'ensemble de ces éléments démontre que tant l'identification que la qualification de l'objet sur lequel se fondent les prétentions de la société Anaphore et M. X. demeurent floues et incompatibles avec la caractérisation nécessaire de l'originalité d'une œuvre de l'esprit au sens du code de la propriété intellectuelle ;

Le jugement sera donc confirmé en ses dispositions relatives au rejet de la protection du droit d'auteur du logiciel Arkhelia ;

La cour,

Confirme le jugement déféré en toutes ses dispositions,

Y ajoutant,

Condamne in solidum la société Anaphore et M. X. à payer la somme de 6 000 euros au conseil départemental de l'Eure, sur le fondement des dispositions de l'article 700 du code de procédure civile, ainsi qu'aux dépens d'appel ;

## TD N°5 PROTECTION DES OEUVRES NUMERIQUES

### 1. LA COMPLEXITE DU DROIT D'AUTEUR APPLICABLE AU JEU VIDEO

= 0 (??)

Annexe 1

L'industrie du jeu vidéo évolue en permanence, à la fois sur le plan créatif (l'apparence des jeux), technologique (le matériel et les logiciels qui donnent vie aux jeux) et commercial (les modèles d'affaires utilisés pour distribuer les jeux aux consommateurs). Toutes ces innovations donnent naissance à de nouveaux enjeux.

Tous les acteurs de l'écosystème du jeu vidéo – développeurs, investisseurs, éditeurs et distributeurs – doivent se préoccuper de certaines questions juridiques fondamentales concernant en particulier la mise en place de dispositions juridiques appropriées pour assurer le développement, le financement et la distribution des jeux. Si la protection de la vie privée, la sécurité des données, la réglementation des contenus et la monétisation sont des considérations incontournables l'élaboration d'une stratégie de propriété intellectuelle dynamique visant à lui assurer des droits appropriés est un élément indispensable au succès de l'entreprise d'un développeur.

**Vous créez un « studio » autour du développement d'un nouveau jeu vidéo sur smartphone dans lequel vous investissez toutes vos économies et décidez de faire appel à  cinq contributeurs autoentrepreneur . Chacun travaille en fonction de sa compétence et de façon libre. En tant que personne à l'initiative du jeu , vous établissez le scénario ainsi que les personnages, une personne travaille sur la musique du jeu et décide de  remixer un morceau célèbre , une deuxième personne travaille sur le graphisme du jeu ainsi que le logo sous lequel sera distribué le jeu, une autre travaille sur l'animation multimédia du jeu, deux autres sur la programmation technique du logiciel et son intégration sachant qu'une partie du code est repris d'un code existant placé sous la licence suivante  CC BY-SA .**

**Vous vous inquiétez du régime juridique à appliquer à votre jeu souvent source d'insécurité. Vous disposez d'un extrait de jurisprudence sur le jeu vidéo en annexe 1 pour vous aider.**

Il faut à présent vous préoccuper des questions juridiques suivantes :

1. Qui sera l'éditeur du jeu ? Pourquoi ?
2. A quelle difficulté principale serez vous confronté en tant qu'éditeur ?
3. Devriez vous considérer le jeu vidéo comme :
  - une oeuvre ?
  - une oeuvre logicielle ?
  - une oeuvre audiovisuelle ?
4. Quel intérêt avez vous à voir reconnaître le jeu vidéo en tant qu'oeuvre collective ?
5. Pensez vous que la jurisprudence actuelle vous donne raison ?
6. Quel régime juridique risque de se voir appliquer le jeu vidéo ?
7. Vous hésitez sur la nature de la collaboration à avoir avec les contributeurs : le statut d'autoentrepreneur des contributeurs change t-il quelque chose dans l'applicabilité du droit d'auteur ?
8. Quelles sont les précautions à prendre en matière de droits de propriété intellectuelle en ce qui va concerner :
  - la musique ?
  - le logiciel ?
9. Comment allez vous protéger le nom et le logo de votre jeu ?
10. Les cinq contributeurs peuvent-ils exiger que vous citiez leurs noms lors de la distribution du jeu ?
11. Que vous inspire l'ensemble de ces questionnements à propos du jeu vidéo ?

## 2. DIRECTIVE EUROPEENNE SUR LE DROIT D'AUTEUR

### Annexe 2

1. Déterminez quel est l'objectif de la directive européenne sur le droit d'auteur ?
  2. Justifiez la nécessité d'une nouvelle directive sur le droit d'auteur ?
  3. Dites quel sont les apports de la directive ?
  4. Reflexion : est ce une forme de censure ou une nécessité pour la protection des auteurs ?
-

## ANNEXE 1 La Cour de cassation tranche sur le statut juridique du jeu vidéo

Publié le 09/08/2009 par Thibault Verbiest, Perrine Pelletier

*La Cour de cassation dans un arrêt du 25 juin 2009 rendu par la 1<sup>re</sup> chambre civile, confirme l'analyse de la cour d'appel de Paris statuant sur le statut juridique du jeu vidéo. La question faisant controverse depuis toujours, cette jurisprudence servira-t-elle de référence ou d'élément déclencheur pour décider le législateur à s'emparer du sujet ?*

Dans cette affaire, la société Cryo, développeur et éditeur de jeux vidéo avait intégré dans ses oeuvres des compositions musicales créées par des auteurs adhérents à la SACEM – société de gestion collective des droits d'auteur dont les droits dans les domaines des oeuvres multimédias sont perçus par la Sesam. Il est reproché à la société Cryo de ne jamais avoir demandé d'autorisation préalable. Il en résultait selon la Sesam un préjudice du fait du défaut de perception de ces redevances. La cour d'appel avait fait droit à cette demande en se fondant sur le statut juridique composite du jeu vidéo, oeuvre complexe.

La jurisprudence avait jusqu'alors été hésitante, préférant d'abord l'assimilation du jeu vidéo à un logiciel (Cass. crim., 21 juin 2000, n° 99-85.154) , pour finalement qualifier le jeu vidéo d'oeuvre multimédia (CA Paris, 2 avr. 2004 : Juris-Data n° 2004-239770) . Par cette décision de 2007, la cour d'appel quant à elle, avait opté pour une solution originale en reconnaissant aux jeux vidéo un régime juridique distributif composé des règles propres aux logiciels et d'autres qui relevaient du droit d'auteur. Ainsi en décide la Cour suprême en réaffirmant la nature juridique complexe du jeu vidéo « qui ne saurait être réduite à sa seule dimension logicielle, quelle que soit l'importance de celle-ci, de sorte que chacune de ses composantes est soumise au régime qui lui est applicable en fonction de sa nature... ».

Il résulte d'abord de cet état de la jurisprudence qu'est dénié aux jeux vidéo le statut d'oeuvres audiovisuelles (not. depuis Cass. 1<sup>re</sup> civ., 28 janv. 2003 : JCP E 2003, p. 588 ) argument pourtant soutenu par la défense. L'intérêt de cette catégorie juridique résidait justement dans le régime propre et adapté aux oeuvres collectives que la société de jeux vidéo revendiquait pour son industrie à la croisée des mondes artistiques et techniques. Par conséquent, à ce jour, le jeu vidéo est qualifié d'oeuvre de collaboration et ce, dès lors que ses compositions (musicales, scéniques, photographiques etc.) ne se fondent pas dans l'ensemble et qu'il reste possible d'attribuer aux compositeurs des droits distincts.

## ANNEXE 2 Droit d'auteur et numérique : les mots pour comprendre la nouvelle directive européenne

Le texte soulève un débat sur les bénéfices ou les dangers qu'il aurait pour la culture sur Internet.

LE MONDE | 12.09.2018 à 16h12 • Mis à jour le 12.09.2018 à 20h00

Le Parlement européen a finalement adopté, mercredi 12 septembre, une directive qui doit adapter le droit d'auteur à l'heure du numérique. Ce vote a lieu après une campagne intense de lobbying à propos de ce texte, dont une première version avait été rejetée par le Parlement en juillet.

Pour les partisans de la directive — industries culturelles, médias, artistes... —, elle est en effet nécessaire pour assurer une meilleure rémunération des créateurs et des éditeurs dans l'économie actuelle d'Internet. Pour les opposants — les grandes entreprises du Web et les défenseurs des libertés numériques —, il s'agit d'un texte européen dangereux à la fois pour leur business et pour leur fonctionnement, ainsi que pour la liberté d'expression.

Pour bien comprendre les enjeux liés à ce texte (qui doit encore être négocié entre la Commission, le Conseil européen et le Parlement européen, avant d'être traduit dans les législations nationales de chaque pays membre de l'UE), voici un lexique des mots et expressions qui reviennent le plus souvent à son sujet.

### Article 11

Cet article de la directive européenne crée le principe d'un « droit voisin » dont pourront se réclamer les entreprises de presse. Il contraint les grandes plates-formes du numérique à rémunérer les médias lorsqu'elles affichent des extraits d'articles ou d'autres contenus sur leurs services.

#### Droits voisins :

Le droit d'auteur est un droit de propriété intellectuelle sur une œuvre de l'esprit. Les « droits voisins du droit d'auteur » peuvent être accordés à des personnes physiques ou morales qui jouent un rôle dans la création de cette œuvre de l'esprit, sans en être directement l'auteur : les entreprises de presse sont concernées, car elles permettent à des journalistes de publier des articles de presse, sans en être directement l'auteur. Celles et ceux qui bénéficient d'un « droit voisin » peuvent toucher des droits patrimoniaux lorsque l'œuvre est utilisée, et ont un droit moral sur le respect de l'œuvre. Ils existent déjà dans la musique pour les artistes interprètes et les producteurs, par exemple.

#### Snippets et « mots individuels » :

Un élément clef des débats sur l'article 11 consiste à définir ce qui constitue, ou non, une « exploitation » d'un article de presse. Le texte adopté vise assez spécifiquement les

« snippets », c'est-à-dire de courts extraits d'un article qui sont affichés par exemple lorsqu'on les partage sur Facebook ou qu'on parcourt Google Actualités. L'article 13 dans la version adoptée mercredi 12 septembre, précise toutefois que les liens seuls ne sont pas concernés, et que ces derniers peuvent être accompagnés de « mentions individuelles » — une notion floue que les Parlements nationaux devront vraisemblablement préciser.

## Article 13

Cet article vise à contraindre les grandes plates-formes d'Internet (Google, Facebook...) à négocier des accords avec les titulaires de droits — ce qui est déjà largement le cas, mais les ayants droit estiment que ces accords leur sont défavorables. À défaut d'accord, les grandes plates-formes devront s'engager à empêcher leurs utilisateurs de publier des contenus protégés par le droit d'auteur.

### Blocage automatique :

Très critiqué, le principe d'un blocage automatique de tous les contenus ne respectant pas le droit d'auteur est déjà en place sur certaines plates-formes, dont YouTube. Ce système, dit « *content ID* », scanne automatiquement les morceaux de musique et les vidéos mis en ligne sur la plate-forme pour y détecter des « signatures numériques », théoriquement uniques et propres à chaque morceau ou vidéo. Lorsque YouTube détecte qu'une vidéo utilise du contenu soumis au droit d'auteur, il la bloque ou, si les ayants droit l'acceptent, laisse la vidéo en ligne, mais reverse une partie des revenus qu'elle génère aux détenteurs originaux des droits.

### Exceptions au droit d'auteur :

Les adversaires de l'article 13 notaient que les systèmes de filtrage automatique ne respectent que très partiellement les droits des internautes sur les exceptions au droit d'auteur. Dans la plupart des pays européens, la loi prévoit notamment des dérogations plus ou moins étendues pour les parodies, les remix, ou le droit de citation.

IUT DE PARIS



Département Informatique  
Economie, Gestion, Organisation et Droit  
DROIT DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

TD N°6 LA LUTTE CONTRE LA CYBERCRIMINALITE

**1. LANCEUR D'ALERTE OU ATTEINTE AU STAD ?**

Annexe 1

1. Présentez les parties, la juridiction saisie et les faits à l'origine du litige.
2. Résumez les griefs formulés à l'égard de l'ex salarié et de l'inspectrice du travail.
3. Dites ce que la loi du 6 décembre 2013 introduit dans le droit du travail et en quoi cela pourrait influencer la décision de la justice.
4. Dites si cela est le cas et justifiez.
5. Énoncez la décision et ses motivations.

## **2. RECHERCHE GOOGLE ET FAILLE DE SECURITE : ATTEINTE AU STAD ?**

Annexe 2

1. Identifiez la juridiction saisie et les parties.
  2. Résumez les faits.
  3. Précisez et justifiez la décision rendue en deux temps.
  4. Que précise cet arrêt sur l'atteinte au STAD ?
-

Il résulte des éléments du dossier et des débats que le 20 décembre 2013, le conseil de la société TEFAL a déposé plainte contre X auprès du Procureur de la République du Tribunal de Grande Instance d'Annecy pour :

- délit d'atteinte au secret des correspondances électroniques,
- délit d'accès et de maintien frauduleux dans tout ou partie d'un système de traitement automatisé de données,
- recel de secret des correspondances et de délit d'accès ou de maintien frauduleux dans tout ou partie d'un système de traitement automatisé de données.

Il expliquait que la société TEFAL disposait d'un système de traitement automatisé de données hébergé par la société Easy à Nanterre et soumis pour maintenance et sécurité à des administrateurs réseau de la société TEFAL exerçant sur RUMILLY et ÉCULLY.

Une charte informatique, dite charte d'utilisation des systèmes d'information et de communication du groupe SEB, définissait les règles d'utilisation et de sécurité ainsi que celles de maintenance, de surveillance et de contrôle. Elle était annexée au règlement intérieur du site de la société TEFAL.

La charte prescrivait notamment « de ne pas utiliser ou essayer d'utiliser des comptes utilisateur autres que le sien ou de masquer sa véritable identité et de ne pas tenter de lire, copier, copier des données dont l'utilisateur n'a pas la responsabilité. » Était plus généralement prohibé « toute utilisation des ressources techniques et informations du groupe qui serait contraire aux lois et règlements en vigueur et toute atteinte à la confidentialité d'un message ou d'une correspondance dont le destinataire est individualisé notamment par sa lecture son interception ou encore son réacheminement non autorisé »

Il résultait de la plainte déposée: que des documents confidentiels établis par Monsieur A. Directeur de Ressources Humaines de la société TEFAL, et des mails émis ou reçus par celui-ci avaient fait l'objet de publications : le 12 décembre 2013, sur le site Internet de la Confédération Nationale du Travail, le 3 décembre 2013 via un compte Facebook et le 12 décembre 2013 par le journal l'humanité. Par la suite d'autres journaux publiaient copie de ces documents.

Une enquête était confiée à la section de recherche de la gendarmerie de Chambéry.

Parallèlement à l'enquête en cours, il était procédé, début janvier 2014, au sein de la société TEFAL, à la saisie en présence d'un huissier de justice, de l'ensemble des disques durs des administrateurs réseaux de la société.

La société TEFAL confiait une expertise de ces disques durs à la société LEXSI expert en informatique, avec mission de procéder à l'audit des postes de travail des personnes possédant des droits d'accès privilégiés sur le système de messagerie de l'entreprise et d'effectuer l'analyse et la recherche de traces numériques des documents litigieux.

Monsieur A. directeur des ressources humaines de la société TEFAL soupçonnait que les faits avaient été commis par un des administrateurs réseau.

L'expertise diligentée par la société LEXSI mettait en évidence la manipulation par Monsieur M. de certains des documents qui avaient été publiés.

Monsieur A. directeur des ressources humaines de la société TEFAL, était réentendu. Il précisait que Monsieur M. était administrateur réseau en charge de différents comptes informatiques permettant l'accès aux services de messagerie, ainsi qu'à des systèmes informatiques à usage professionnel de l'entreprise. Il avait ainsi connaissance d'environ 800 mots de passe de l'entreprise.

Monsieur D., expert réseau sécurité, confirmait que Monsieur M. avait la possibilité de se connecter sur une voie de contrôle d'administration qui lui permettait d'avoir accès aux boîtes mail de l'entreprise.

Monsieur M., entendu le 10 avril 2014 par la Section de Recherche de la Gendarmerie de Chambéry, expliquait avoir été embauché par la société TEFAL en 1994, avoir intégré le service informatique du groupe à RUMILL Y en 1995 en tant que technicien micro, pour évoluer en 2001 en tant qu'administrateur système, puis administrateur infrastructure réseau.

Il expliquait que son rôle consistait à développer plus particulièrement le WIFI qu'il disposait des droits d'administrateur et qu'il lui arrivait de créer des comptes utilisateurs.

Il affirmait détenir les droits pour accéder à tous les serveurs de fichiers mais pas pour les boîtes mail.

Monsieur M. expliquait qu'il était en conflit avec son entreprise pour le paiement des heures supplémentaires ayant vainement tenté d'obtenir leur paiement ainsi qu'un rendez-vous avec Monsieur A. Il déclarait avoir trouvé le 16 octobre 2013 dans une imprimante utilisée par les services des ressources humaines un document dans lequel il apparaissait que le groupe TEFAL avait l'intention de le licencier en utilisant des moyens déloyaux.

Il avait décidé, une quinzaine de jours après, de consulter les serveurs de fichiers RUM17NT à la recherche de documents qui auraient pu le concerner, car ces serveurs de fichiers abritaient toutes les données des documents partagés au sein de la société TEFAL.

Il s'était rendu dans le répertoire des ressources humaines et avait découvert un document intitulé « capteurs sociaux » sur lequel figurait le nom de l'inspectrice du travail et de son supérieur ainsi que des éléments la concernant.

Monsieur M. indiquait avoir décidé alors de faire une copie écran par des manipulations de copier-coller sur son PC, puis avoir effacé le document après l'avoir copié sur la carte SD de son téléphone portable.

Il ajoutait que le même jour, au cours de sa recherche, il avait aussi découvert un document informatique intitulé « msg » qu'il avait également copié, précisant « je savais que je n'aurais pas dû ».

Monsieur M. admettait avoir pénétré dans le système automatisé de traitement de données de la société TEFAL à la recherche d'éléments le concernant et consulté les serveurs de fichiers RUM17NT sans lien avec sa fonction, s'y est maintenu dans une intention autre que celle d'exécuter son travail habituel de développement du WIFI.

Monsieur M. affirmait avoir gardé ces documents plusieurs semaines, puis, après, avoir consulté le site internet de l'inspection du travail pour trouver les coordonnées de l'inspectrice concernée. Il lui avait adressé un message sur sa boîte mail professionnelle lui indiquant qu'il avait « trouvé des documents qui laissaient entendre que la direction de la société TEFAL exerçait des pressions sur elle, par l'intermédiaire de son supérieur. Je lui ai indiqué que j'avais en ma possession les copies d'écran de ces documents et que je pouvais les lui transmettre sur une boîte mail autre que sa boîte professionnelle ». Celle-ci lui ayant répondu en lui communiquant son adresse personnelle, il lui avait adressé les documents sur cette boîte mail après avoir créé lui-même une boîte mail à cette seule fin.

Monsieur M. indiquait avoir refusé de lui communiquer son identité ajoutant que l'inspectrice lui avait indiqué pouvoir éventuellement le protéger.

Il avait appris en fin d'année 2013 par divers collègues qu'un article de l'humanité faisait état des documents qu'il avait fournis.

Monsieur M. affirmait qu'il n'avait pas imaginé que l'inspectrice allait tout diffuser à la presse ajoutant que si c'était à refaire il n'aurait pas copié ces documents.

Madame J. épouse P. était entendue le 24 juin 2014 par la Section de Recherche de la Gendarmerie de CHAMBERY. Elle indiquait être arrivée à ANNECY en qualité d'inspectrice du travail en janvier 2012 sur un secteur territorial défini dans lequel se trouvait notamment la société TEFAL.

Elle déclarait avoir rencontré des difficultés avec sa hiérarchie en la personne de son directeur Monsieur D. Elle expliquait qu'à la suite des entretiens avec celui-ci notamment celui du 18 avril 2013, elle avait été particulièrement affectée. Elle s'estimait victime de sa part d'un harcèlement moral destiné à la faire changer dans son mode relationnel avec la société TEFAL. Monsieur D. lui reprochant sa trop grande rigidité notamment à l'égard de la société TEFAL lui prédisait des difficultés dans sa carrière.

Au cours de son arrêt de travail, elle avait reçu un appel téléphonique de sa secrétaire lui indiquant la réception, sur sa boîte mail professionnelle, d'un mail « bizarre » la concernant. Celle-ci le lui avait transféré sur sa boîte mail personnelle.

Madame J. affirmait avoir détruit ce mail dans lequel l'auteur lui indiquait « qu'il avait des documents probants, comme quoi il pouvait me prouver que TEFAL avait une implication dans ma situation personnelle ».

Elle avait contacté l'auteur afin qu'il lui fasse parvenir les documents.

Elle précisait qu'il s'agissait d'un fichier Excel et pour le mail d'une capture d'écran et qu'elle avait encore reçu d'autres documents notamment des mails échangés entre son directeur et Monsieur A. ainsi qu'un mail échangé entre Monsieur A. et Madame R. la responsable des ressources humaines de TEFAL à RUMILLY.

Madame J. expliquait avoir directement saisi le Conseil National de l'inspection du Travail début décembre 2013 par un courrier avec accusé de réception pour atteinte à son indépendance et avoir transmis tous les documents reçus.

Elle avait aussi mis en copie et transmis copie de ces documents aux organisations syndicales du département : la CNT, le SNU, la CGT, FO, la CFDT, INSA et SUD.

Lors de son audition le 24 juin 2014, elle déclarait, au sujet de la diffusion de ces documents sur les sites internet et dans la presse, qu'il s'agissait d'un problème qui venait de TEFAL et qu'elle avait juste fait son travail.

*S'agissant du statut de lanceur d'alerte :*

*L'article L1132-3-3 du Code du Travail prévoit qu'aucune personne ne peut être écartée d'une procédure de recrutement ou de l'accès à un stage ou à une période de formation en entreprise, aucun salarié ne peut être sanctionné, licencié ou faire l'objet d'une mesure discriminatoire, directe ou indirecte, notamment en matière de rémunération, au sens de l'article L. 3221-3, de mesures d'intéressement ou de distribution d'actions, de formation, de reclassement, d'affectation, de qualification, de classification, de promotion professionnelle, de mutation ou de renouvellement de contrat, pour avoir relaté ou témoigné, de bonne foi, de faits constitutifs d'un délit ou d'un crime dont il aurait eu connaissance dans l'exercice de ses fonctions.*

*En cas de litige relatif à l'application du premier alinéa, dès lors que la personne présente des éléments de fait qui permettent de présumer qu'elle a relaté ou témoigné de bonne foi de faits constitutifs d'un délit ou d'un crime, il incombe à la partie défenderesse, au vu des éléments, de prouver que sa décision est justifiée par des éléments objectifs étrangers à la déclaration ou au témoignage de l'intéressé. Le juge forme sa conviction après avoir ordonné, en cas de besoin, toutes les mesures d'instruction qu'il estime utiles.*

*Ce texte relatif au droit du travail a été créé par la loi du 06 décembre 2013 soit postérieurement aux faits.*

Monsieur M. aurait pu, après décembre 2013, ébranlé à la lecture du document attestant de l'intention de la société TEFAL de le licencier, utiliser ultérieurement ce document, qu'il a affirmé avoir trouvé par hasard dans la photocopieuse, dans le cadre d'une procédure prudhomale. S'agissant des documents obtenus par celui-ci à la suite de son intrusion dans le système de traitement automatisé de la société TEFAL, il n'en a pas eu connaissance dans l'exercice de ses fonctions, ils ne le concernaient pas personnellement et n'étaient pas nécessaires à l'exercice de sa défense dans un cadre prudhomal.

Sur les faits reprochés à Madame J. épouse P. :

Sur le recel de correspondance électronique et de données internes à la société Tefal provenant du délit d'interception de détournement d'utilisation ou de divulgation de mauvaise foi de correspondances émises transmises reçues par voie électronique ; Madame J. épouse P. a été contactée, sur sa boîte mail professionnelle par Monsieur M. de manière anonyme alors qu'elle se trouvait en arrêt maladie. Sa secrétaire, interpellée par le caractère « bizarre » du mail l'a contactée téléphoniquement et lui a transféré ce mail sur sa boîte personnelle. Elle affirme que les mails lui ont été transmis sur sa boîte mail personnelle intitulée pl@yahoo.fr. Monsieur M. souvenant lui d'une boîte mail se terminant par alice.fr. En tout état de cause aucun de ces échanges de mails ne semblent avoir été conservé par les protagonistes qui ont préféré les supprimer. Madame J. épouse P. confirme avoir été destinataire des copies de mails provenant de la boîte mail de Monsieur A.

Elle ne pouvait ignorer, tant par le contenu des mails, que par l'identité des destinataires, qu'ils avaient été obtenus sans l'accord des titulaires des boîtes mail ; l'évidence de cette connaissance est renforcée par l'organisation de leur envoi anonyme.

La connaissance de la provenance douteuse des documents et le fait qu'elle les ait utilisés suffit à caractériser l'élément intentionnel de l'infraction de recel. L'infraction de recel de détournement de correspondance électronique apparaît en conséquence constituée.

Sur les faits de violation du secret professionnel :

L'article 226-13 du code pénal prévoit que la révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 euros d'amende.

Madame J. épouse P. inspectrice du travail est, comme tout fonctionnaire, tenu au respect des dispositions de l'article 26 de la loi du 13 juillet 1983 qui rappelle l'obligation de respecter le secret professionnel.

Il résulte des règles déontologiques applicables à la profession d'inspecteur du travail que pour l'inspection du travail le secret professionnel a pour objet dans l'intérêt des personnes de garantir la sécurité des confidences recueillies et de protéger les informations à caractère secret auxquelles elle a accès ».

Madame J. épouse P. a estimé à la lecture des documents qui lui avaient été communiqués à titre personnel, sous couvert de l'anonymat, qu'ils attestaient de pressions de la société TEFAL à son encontre, qu'ils étaient des éléments d'information nécessaires dans le conflit qui l'opposait à son supérieur hiérarchique et qu'ils devaient être portés à la connaissance du CNT qu'elle avait décidé de saisir.

Elle a ajouté dans son audition qu'elle avait dressé procès-verbal estimant que des infractions pénales étaient caractérisées. Pourtant elle n'avait pas encore, le 24 juin 2014 lors de celle audition, soit plus de six mois après la réception des documents, saisi le Procureur de la République des infractions qu'elle affirme constituées ; alors qu'elle avait transmis, dès décembre 2013, à sept organisations syndicales l'ensemble de ces documents.

Elle a, en outre, prétendu à tort dans son audition devant les services de gendarmerie que cette diffusion avait été faite en application d'un article du code du travail.

Cette diffusion aux organisations syndicales a rendu possible la publication dans la presse et sur internet de ces documents internes à la société TEFAL, diffusion qui a conduit à l'identification de Monsieur M. et à son licenciement de la société TEFAL.

Cette large diffusion, qui ne se limite pas à la simple diffusion à l'éventuelle organisation syndicale chargée de défendre ses propres intérêts, ne saurait s'apparenter à l'exercice des droits de la défense déjà pleinement mis en oeuvre par la saisine du CNT, où siègent des représentants d'organisations syndicales. Elle atteste d'un choix délibéré de communiquer des documents secrets et internes à une entreprise, avec une volonté de large diffusion, qui dépasse l'échelon individuel.

Madame J. épouse P. ne saurait de ce fait invoquer un quelconque fait justificatif tiré de l'exercice des droits de la défense.

Les faits de violation du secret professionnel apparaissent caractérisés.

Quant au statut de lanceur d'alerte :

L'article L 1132-3-3 du Code du Travail a été créé par la loi du 06 décembre 2013 postérieurement aux faits.

Les documents diffusés aux organisations syndicales par Madame J. épouse P. n'ont pas été obtenus dans le cadre de l'exercice de ses fonctions, ils n'ont pas été utilisés dans le strict exercice de sa défense et il n'est pas établi qu'ils constituent un crime ou un délit.

En conséquence le délit de violation du secret professionnel apparaît constitué.

Les faits reprochés à Madame J. épouse P. sont établis. {...}

## DECISION

### SUR L'ACTION PUBLIQUE :

Déclare M. C. coupable des faits qui lui sont reprochés.

Pour les faits de ATTEINTE AU SECRET DES CORRESPONDANCES EMISES PAR VOIE ELECTRONIQUE commis du 1er octobre 2013 au 31 décembre 2013 à RUMILLY (74)

Pour les faits de ACCES FRAUDULEUX DANS UN SYSTEME DE TRAITEMENT AUTOMATISE DE DONNEES commis du 1er octobre 2013 au 31 décembre 2013 à RUMILLY (74)

Pour les faits de MAINTIEN FRAUDULEUX DANS UN SYSTEME DE TRAITEMENT AUTOMATISE DE DONNEES commis du 1er octobre 2013 au 31 décembre 2013 à RUMILLY (74)

Condamne M.C. au paiement d'une amende de trois mille cinq cents euros (3 500 euros) ;

Déclare J. L. épouse P. coupable des faits qui lui sont reprochés.

Pour les faits de RECEL DE BIEN PROVENANT D'UN DELIT PUNI D'UNE PEINE N'EXCEDANT PAS 5 ANS D'EMPRISONNEMENT commis du 1er octobre 2013 au 31 décembre 2013 à ANNECY (74)

Pour les faits de VIOLATION DU SECRET PROFESSIONNEL commis du 1er octobre 2013 au 31 décembre 2013 à ANNECY (74)

Condamne J. L. épouse P. au paiement d'une amende de trois mille cinq cents euros (3 500 euros) ;{...}

**SUR L'ACTION CIVILE:**

Déclare recevable les constitutions de partie civile de la SAS TEFAL

Condamne M. C. et J. L. épouse P. à payer solidairement :

-la somme de un euro (1 euro) au titre de dommages-intérêts à la SAS TEFAL, partie civile, pour tous les faits commis à son encontre,

En outre, condamne M. C. et J. L. épouse P. à payer solidairement à la SAS TEFAL., parties civiles, la somme de 2 500 euros au titre de l'article 475-1 du code de procédure pénale ;

*Cette décision est frappée d'appel.*

## PROCÉDURE

## La saisine du tribunal et la prévention

O. L. été convoqué le 11 février 2013 devant le tribunal de grande instance de Créteil par officier de police judiciaire sur instructions du procureur de la République pour :

1/ avoir à Maisons-Alfort, Orléans, dans le département du Val de Marne, du 1er août 2012 au 3 septembre 2012, en tout cas sur le territoire national et depuis temps non prescrit, accédé frauduleusement à tout ou partie d'un système de traitement automatisé de données, en l'espèce de l'extranet de l'Agence Nationale de Sécurité Sanitaire de l'Alimentation, de l'Environnement et du Travail (Anses), infraction prévue par l'article 323-1 al. 1 du code pénal et réprimée par les articles 323-1 al. 1, 323-5 du code pénal,

2/ s'être à Maisons-Alfort, Orléans, dans le département du Val de Marne, du 1er août 2012 au 3 septembre 2012, en tout cas sur le territoire national et depuis temps non prescrit, maintenu frauduleusement dans tout ou partie d'un système de traitement automatisé de données, en l'espèce de l'extranet de l'Agence Nationale de Sécurité Sanitaire de l'Alimentation, de l'Environnement et du Travail (Anses), infraction prévue par l'article 323-1 al. 1 du code pénal et réprimée par les articles 323-1 al. 1, 323-5 du code pénal,

3/ avoir à Maisons-Alfort, Orléans, dans le département du Val de Marne, du 1er août 2012 au 3 septembre 2012, en tout cas sur le territoire national et depuis temps non prescrit, frauduleusement soustrait des documents sur l'extranet de l'Agence Nationale de Sécurité Sanitaire de l'Alimentation, de l'Environnement et du Travail (Anses), données téléchargées puis fixées et enregistrées sur plusieurs supports (média center et disque dur), au préjudice de l'Anses, infraction prévue par les articles 311-1, 311-3 du code pénal et réprimée par les articles 311-3, 311-14 1°, 2°, 3°, 4°, 6° du code pénal.

## Le jugement :

Le tribunal de grande instance de Créteil, 11ème chambre, par jugement contradictoire, en date du 23 avril 2013, a relaxé O. L. des fins de la poursuite.

[...]

## FAITS

Rendue après en avoir délibéré conformément à la loi,  
Statuant sur l'appel régulièrement interjeté par le ministère public à l'encontre du jugement déféré.

Les faits à l'origine des poursuites sont les suivants :

Le 6 septembre 2012, l'Agence Nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail (Anses), opérateur d'importance vitale (OIV), déposait une plainte auprès des services de police de Maisons-Alfort, après la détection, le 3 septembre 2012, d'un accès frauduleux sur son serveur extranet.

Cette détection faisait suite à la découverte d'un article relatif aux nano-matériaux mis en ligne sur le site d'information alternatif "reflets info", article accompagné d'un document de travail "powerpoint" appartenant à l'agence destiné uniquement à un usage restreint.

Cet article consacré à la dangerosité des nano-matériaux était signé d'une personne utilisant le pseudonyme "Yovan M."

Les enquêteurs relevaient qu'un extranet constitue une extension d'un réseau interne à une entité, à la différence d'un site internet, vers des partenaires situés hors du réseau. Cet accès se fait via internet par une connexion sécurisée avec un mot de passe dans la mesure où cela offre un accès au système d'information à des personnes situées en dehors de l'entité, à la différence d'un intranet.

L'Anses constatait que de nombreux documents (8000 fichiers) situés dans un dossier "lecture" avaient été exfiltrés les 27 et 28 août 2012 vers une adresse IP d'un VPN (réseau privé Virtuel) localisée au Panama. Leur auteur avait profité d'une faille de sécurité dans les paramètres du serveur extranet concernant l'identification en permettant l'accès. L'accès était ainsi rendu possible par l'utilisation de l'URL complète.

Les investigations menées permettaient la découverte d'un second article relatif à la légionellose signé par un individu utilisant le surnom "Bluetouff", accompagné d'un fichier compressé contenant des documents provenant dudit serveur extranet. Le même "Bluetouff" indiquait aussi être en possession de 7,7 gigaoctets de documents traitant de questions de santé publique.

L'analyse des journaux de connexion du serveur extranet et du firewall de l'Anses confirmait la primo-analyse réalisée par l'Anses concernant la localisation des adresses IP ayant exfiltré un volume important de fichiers appartenant à l'agence. Si une adresse correspondait à un service VPN suédois dont le propriétaire ne pouvait être identifié, une seconde adresse IP ayant effectué un téléchargement de 82 Go de données entre le 27 et le 28 août 2012 était localisée au Panama. Cette adresse IP provenait d'un serveur informatique hébergeant une solution VPN de la société "Toonux.net", fondée et dirigée par O. L.

Celui-ci était par ailleurs identifié comme étant l'internaute utilisant l'alias "Bluetouff".

Lors de ses auditions par les enquêteurs, O. L. reconnaissait avoir récupéré via son VPN panaméen l'ensemble des données litigieuses stockées sur le serveur extranet de l'Anses. Il déclarait avoir découvert tous ces documents en libre accès après une recherche complexe sur le moteur de recherche Google.

S'il affirmait être arrivé "par erreur" au cœur de l'extranet de l'Anses, il reconnaissait néanmoins avoir parcouru l'arborescence des répertoires de celui-ci et être remonté jusqu'à la page d'accueil sur laquelle il avait constaté la présence de contrôles d'accès (authentification par identifiant et mot de passe).

Il précisait ne pas avoir diffusé l'archive de 7,7 gigaoctets qu'il avait générée et en avoir seulement fait une extraction de 250 megaoctets qu'il avait utilisée pour argumenter son article sur la légionellose.

Il admettait avoir communiqué des documents à un autre rédacteur du site "Reflets. info", à savoir "Yovan M.", identifié comme étant Pascal H.

Les investigations techniques menées lors de la perquisition réalisée au domicile d'O. L. permettaient la récupération de l'archive complète de 7,7 Go. Il acceptait par ailleurs de retirer les fichiers et liens de téléchargement en rapport avec les documents appartenant à l'Anses sur l'ensemble des serveurs et supports.

Pascal H. confirmait avoir eu accès aux données de l'Anses et avoir utilisé un fichier sur la thématique des "nano-argents" pour illustrer un article. Il reconnaissait en outre avoir rendu public ce fichier sur un site de téléchargement, sachant que les documents provenaient de la documentation de l'Anses. Mais il indiquait ignorer qu'ils avaient été collectés sur un espace privé. Il retirait le fichier "Piano Etat des Lieux 2012" de l'espace d'hébergement en ligne utilisé.

A l'audience publique de la cour, O. L. comparait assisté. Il indique vivre en concubinage, être père d'un enfant âgé de 5 ans, percevoir, comme développeur informateur salarié un revenu mensuel de 2011 €.

Le ministère public requiert l'infirmité du jugement et la condamnation du prévenu à une peine d'amende de 5000 € en partie assortie du sursis.

Le conseil du prévenu développe les conclusions de relaxe qu'il a déposées et qui ont été visées par le président et le greffier. Il demande, estimant que les infractions ne sont pas caractérisées, de confirmer le jugement sur les relaxes prononcées en première instance, à titre subsidiaire de prononcer un ajournement du prononcé de la peine et, en cas de condamnation, de dire que la décision ne sera pas mentionnée au casier judiciaire.

#### DISCUSSION :

Considérant qu'il n'est pas établi suffisamment par les pièces de la procédure que le prévenu s'est rendu coupable d'accès frauduleux dans un système de traitement automatisé de données ; que l'accès, qu'il ne conteste pas, lui a en fait été permis en raison d'une défaillance technique concernant l'identification existant dans le système, défaillance que reconnaît l'Agence Nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail ; que dans ces conditions l'infraction n'est pas caractérisée ; qu'il y aura lieu de confirmer le jugement de ce chef ;

Considérant, pour ce qui concerne les faits commis de maintien frauduleux dans un système de traitement automatisé de données et de vol, qu'il est constant que le système extranet de l'Agence Nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail n'est normalement accessible qu'avec un mot de passe dans le cadre d'une connexion sécurisée, que le prévenu a parfaitement reconnu qu'après être arrivé "par erreur" au cœur de l'extranet de l'Anses, avoir parcouru l'arborescence des répertoires et être remonté jusqu'à la page d'accueil, il avait constaté la présence de contrôles d'accès et la nécessité d'une authentification par identifiant et mot de passe ; qu'il est ainsi démontré qu'il avait conscience de son maintien irrégulier dans le système de traitement automatisé de données visité où il a réalisé des opérations de téléchargement de données à l'évidence protégées ; que les investigations ont démontré que ces données avaient été téléchargées avant d'être fixées sur différents supports et diffusées ensuite à des tiers ; qu'il est, en tout état de cause, établi qu'O. L. a fait des copies de fichiers informatiques inaccessibles au public à des fins personnelles à l'insu et contre le gré de leur propriétaire ; que la culpabilité d'O. L. sera donc retenue des chefs de maintien frauduleux dans un système de traitement automatisé de données et de vol de fichiers informatiques au préjudice de l'Agence Nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail (Anses) ;

Considérant que tenant compte de la nature et de la gravité des faits commis, de l'absence d'antécédent judiciaire du prévenu et des éléments connus de sa personnalité, la cour prononcera à son encontre une peine délictuelle de 3000 € ;

Que la demande du prévenu de non inscription au bulletin n°2 de son casier judiciaire de la condamnation sera rejetée, ce dernier ne justifiant pas actuellement de la nécessité d'une telle dispense ;

#### DÉCISION :

Statuant publiquement et contradictoirement à l'encontre d'O. L., prévenu,

- . Déclare recevable l'appel du ministère public,
  - . Infirme partiellement le jugement sur la déclaration de culpabilité,
  - . Déclare O. L. coupable des faits qui lui sont reprochés de maintien frauduleux dans un système de traitement automatisé de données et de vol dans les termes de la prévention,
  - . Confirme pour le surplus sur la culpabilité,
- En répression,
- . Le condamne à une amende délictuelle de 3000 €,
  - . Rejette la demande de dispense d'inscription de la présente condamnation au bulletin n°2 du casier judiciaire d'O. L.

Sem 4

## DROIT DE L'INFO

1  
TD

1) Alexandre : Auteur de la vidéo  
Amis d'Alexandre : Éditeurs  
Le professeur : La victime  
Les plateformes : Hébergeurs  
Parents d'Alexandre : Responsable ~~parents~~ civils

2) Alexandre et ses parents sont responsables. Les amis d'Alexandre sont responsables.  
Les plateformes sont responsables si elle ne supprime pas de contenu après demande.

3) 1 an de prison + 45 000 €  
+ dommages et intérêts.

# 1. LIEN HYPERTEXTE

1) Un photographe a autorisé un site à mettre en ligne sa photo. Une élève d'un lycée. Une étudiante a utilisé cette image et elle a été repus sur le site de l'école.

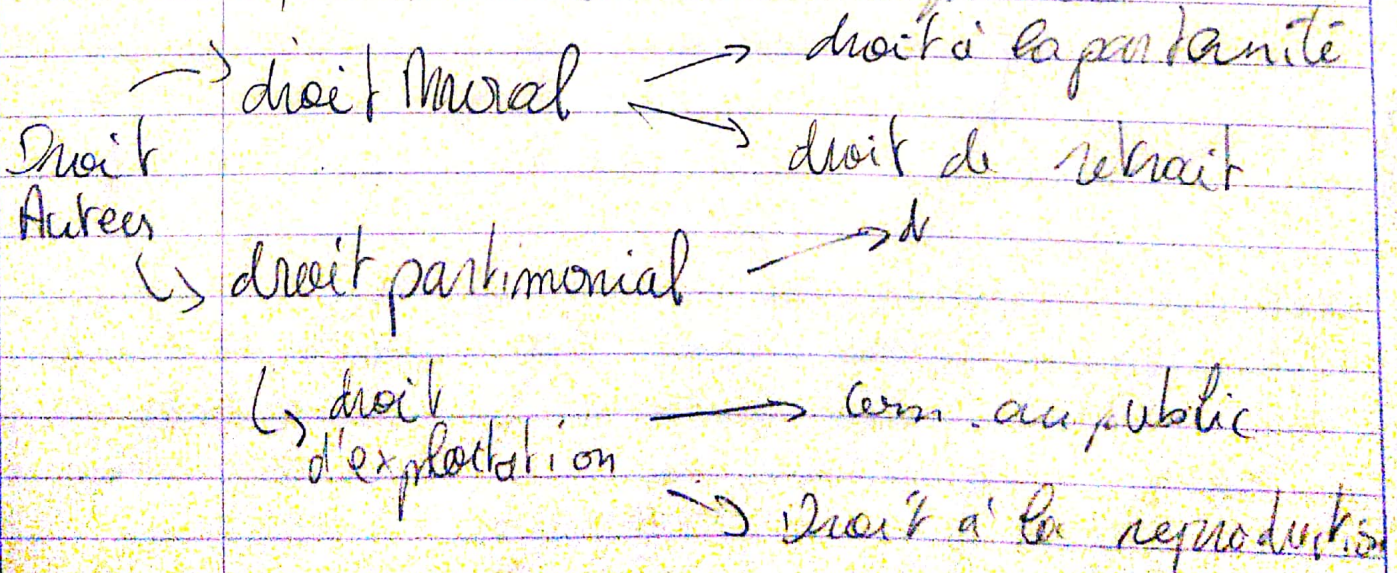
L'auteur de la photo a assigné en justice l'établissement scolaire pour atteinte à ses droits d'auteur sur la photo.

Il demande la cessation du trouble + répar

2) La cour fédérale de justice allemande a saisi la CJUE car elle se posait le problème de droit suivant:

"Le fait de recopier un contenu disponible sur un site avec la permission de l'auteur pour le mettre en ligne sur un autre site sans la permission de l'auteur constitue il une nouvelle communication au public.

3) La communication au public:



4) Le droit à la communication au public est une prérogative exclusive du droit patrimonial d'un auteur.

6) Qui la CDE statut qu'il s'agit d'une nouvelle communication au public en soulignant le fait qu'il ne s'agit pas du même public.

5) Si le site de l'éceeb avait mis un lien vers l'image

## II

1) Juridiction - Cour d'Appel de Douai  
Appelant : Anaphore et M. X  
Intimé : Conseil Départementale de l'Èure

2) Le conseil Départemental de l'Èure une licence d'utilisation pour un bureau de gestion des archives de la société Anaphore. Il lance ensuite une procédure de marché public pour une solution globale d'archivage et ditait ses besoins dans un CCTP.

Anaphore lui reproche de décider trop précipitamment son logiciel et de divulguer son savoir faire à la concurrence

3) Il y a reproduction

4) Est une reproduction

5) Non car c'est pas original → une œuvre

sem 6

## DROIT DE L'INTO

1  
TD

1) L'éditeur a financé, car on supporte financièrement le projet et on a l'initiative

2) Versus des droits d'auteur, les quelles

3) Œuvre

Œuvre : originalité (effort intellectuel d'auteur et/ou empreinte de la personnalité de l'auteur).

Œuvre Logicielle : On ne peut résumer un jeu vidéo à une œuvre logicielle car un centième des images du jeu.

Œuvre Audiovisuelle : On ne peut résumer un jeu à une œuvre audiovisuelle car il est interactif.

4) Cela signifie juridiquement qu'on ne sait pas qui fait quoi. Donc l'auteur est l'éditeur il bénéficie donc des droits patrimoniaux. (F)

5) Non, ce n'est pas une œuvre collective mais de collaboration pour la jurisprudence (on peut distinguer les apports de chaque contributeur).

6) Le régime périodique du jeu vidéo est distributif, chacun dispose des droits patrimoniaux chacun à son tour d'œuvre. Ils sont entrepreneurs dans les domaines ils ne créent pas des droits patrimoniaux

8) Ce qui pose problème, c'est qu'il faut l'accord des ayants droits de la musique (droit à l'intégrité de l'œuvre).

Mais s'ils étaient salariés, leurs droits patrimoniaux nous reviendraient.  
1) La licence du code doit être la même que celui code récupéré

9) Yes leposer depuis de l'INPI

10) Oui ils peuvent l'exiger

11) Le régime du jeu vidéo est extrêmement complexe

## Exercice 2

1) Remancier les auteurs.

2) La directive actuelle sur le droit d'auteur date de 2001. Elle est pas du tout à jour

3) Crie un droit pat. inédit, le droit   
 de son

Criminal

1) La juridiction saisie est le Tribunal Correctionnel (Tribunal) à l'administration. En ce qui concerne la partie, le demandeur est TEFAL, les défendeurs sont Monsieur Meek et Madame Meek.

2) Monsieur A sorti chez des ressources du Monsieur M, administrateur système de TEFAL et trouve un document le concernant dans la photocopieuse et abstrique qu'on veut le passer à la suite pour le licencié. Il va faire dans le serveur et récupère des documents le concernant et fait des copies sur mail et se rend compte de confidentialité entre son entreprise et l'inspection de travail. Elle des transmet à l'ensemble des syndicalistes qui les transmettent à la presse et mention.

TEFAL reproche à M.M l'accès à un système la copie de donnée et à M.J le recel de ces données et violation de secret pro.

3) Cela a traduit le statut de lanceur d'alerte.

4) Non ça n'a rien changé en raison de la non rétro-activité des lois et parce qu'il a récupéré les informations hors de l'exercice de ces fonctions.

Il aurait dû tenter une action en prud'hommes au lieu de faire ça. Le fait qu'il ait été éradiqué à la lecture du doc sur son licenciement il y a donc circonstance d'Atténuation.

5) Il est condamné pour :

- Violation du secret des correspondances
- Accès et maintien dans un SI

Elle est condamnée pour :

- Violation du secret pro
- Accès d'information.

## Exercice

1) La juridiction est le cours d'Appel (du Tribunal correctionnel)  
Appelant: Procureur  
Intimés: O.L.

2) O.L. entre par hasard sur le site de l'Amis et en parcourt l'annuaire et se rend compte qu'il y a un système de sécurité. Il se retourne alors dans le système pour copier des données. Il en communique une partie à un ami qui le publie

Sem 7

## DROIT DE L'INFO

4

TD

C. Anses est un DIV. et lance donc une enquête. Le coupable est retrouvé et il y a dépôt de plainte (Accès maintient et copie). Il est relaxé en 1<sup>ère</sup> instance.

3) Il est condamné pour maintient frauduleux et vol de donnée

4) L'accès peut ne pas être frauduleux mais le maintient oui