

La révolution des drones est-elle conciliable avec la protection de la vie privée et le traitement des données ?

Mémoire réalisé par
Nicolas Orban

Promoteur(s)
Alexandre Cruquenaire

Année académique 2014-2015
Master en droit

Plagiat et erreur méthodologique grave

Le plagiat entraîne l'application des articles 87 à 90 du règlement général des études et des examens de l'UCL.

Il y a lieu d'entendre par « plagiat », l'utilisation des idées et énonciations d'un tiers, fussent-elles paraphrasées et quelle qu'en soit l'ampleur, sans que leur source ne soit mentionnée explicitement et distinctement à l'endroit exact de l'utilisation.

La reproduction littérale du passage d'une oeuvre, même non soumise à droit d'auteur, requiert que l'extrait soit placé entre guillemets et que la citation soit immédiatement suivie de la référence exacte à la source consultée.*.

En outre, la reproduction littérale de passages d'une oeuvre sans les placer entre guillemets, quand bien même l'auteur et la source de cette oeuvre seraient mentionnés, constitue une erreur méthodologique grave pouvant entraîner l'échec.

* A ce sujet, voy. notamment <http://www.uclouvain.be/plagiat>.

REMERCIEMENTS

Maître Alexandre Cruquenaire, mon promoteur,

Maître Pauline Orban,

Monsieur Greg Billen,

Monsieur Patrick Mascart,

Madame Diane Hennebert,

Mes parents, pour leur soutien et leurs encouragements.

TABLE DES MATIERE

Remerciements.....	2
Table des matière	3
Introduction.....	5
Partie I : La vie privée.....	7
Chapitre I : L'étendue de la vie privée.....	8
Section I. La vie privée de l'individu.....	8
Section II. La vie familiale.....	9
Section III. Le domicile	9
Section IV. Le respect de la correspondance	10
Section V. Les données à caractère personnel	10
Section VI. Le droit à l'image.....	11
Section VII. Qui sont les bénéficiaires de la protection de la vie privée ?	12
Chapitre II : Les sources du droit à la vie privée	12
Section I. Droit international.....	12
A. Le droit du Conseil de l'Europe.	13
B. Le droit communautaire.....	15
Section II. Droit belge.....	23
A. La Constitution belge.....	23
B. La loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.	24
C. La loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance.	30
D. La loi du 13 juin 2005 relatives aux communications électroniques.	34
E. Articles 47sexies et 47septies du Code de procédure pénal.	35
Section III. La jurisprudence.....	35
A. Nature et contenu du droit à l'image	36
B. La personne est reconnaissable.....	37
C. Le consentement exprès.....	38
D. Limites au droit à l'image	39
Conclusion sur le droit à l'image jurisprudentiel.....	41
Partie II : Les capacités des drones	42
Chapitre I : Les opérateurs commerciaux	43
Section I. Inspection d'infrastructures	43
Section II. Autres services visuels	44
Section III. Usage à fin de cartographie.....	44
Section IV. Observation de la terre.....	45
Section V. Agriculture	46
Section VI. Utilisations nouvelles.....	46
Chapitre II : Les forces de l'ordre et les autorités étatiques	46
Section I. La surveillance de personnes.....	47
Section II. Protection civile.....	48
Section III. Application de la loi.....	48
Chapitre III : Le journalisme et le cinéma	49
Chapitre IV : Les fournisseurs de télécommunications	49

Chapitre V : L'utilisation de drones par les particuliers	50
Partie 3 : Interactions entre la vie privée et les drones, la protection est elle	
suffisante ?	51
Chapitre I : Menaces, législations et carences	51
Section I. Les opérateurs commerciaux	51
Section II. Les journalistes ou l'utilisation de drones à des fins artistiques	52
Section III. Les autorités de l'Etat	53
Section IV. Les particuliers.....	55
Chapitre II : Proposition de règlement.....	56
Section I. L'introduction du principe de responsabilité.....	56
Section II. Les trois améliorations découlant du <i>soft law</i>	57
A. Le principe de protection des données dès la conception (Privacy by Design) et par défaut (Privacy by Default)	58
B. L'analyse d'impacts relatifs à la vie privée	60
C. L'audit privé	62
Section III. Reconnaissance d'un droit à l'oubli.....	62
Chapitre III : Droit comparé	63
Section I. La législation française.....	63
A. Cadre juridique	63
B. Protection de la vie privée	64
Section II. La législation américaine	66
A. Pour les drones commerciaux ou privés	67
B. Les drones gouvernementaux	67
Chapitre IV : Améliorations possibles du cadre juridique des drones.....	69
Section I. Les professionnels	69
A. La licence.....	69
B. L'assurance	70
C. Manuel d'exploitation et analyse d'impacts	70
D. Mesures de sécurité	71
E. Devoirs et responsabilité de l'exploitant	72
Section II. Les particuliers	72
A. Limitations techniques.....	72
B. Responsabilité.....	73
Section III. Mesures générales envisageables pour compléter le cadre juridique régissant les drones	73
A. Territoire survolable	73
B. Améliorations tirées du droit communautaire	73
C. Améliorations tirées du droit comparé.....	75
D. Autres mesures techniques de prévention	75
Conclusion	76
- Annexe 1 -	80
- Annexe 2 -	84
Bibliographie.....	88

INTRODUCTION

Aéronefs controversés, les drones font souvent la une de l'actualité, notamment avec leurs frappes militaires. Le 7 mai dernier encore, *La libre* annonçait que l'homme qui avait revendiqué les attaques contre Charlie Hebdo fut tué par une frappe de drone américain au Yémen¹. On se souvient aussi des drones qui ont survolé la centrale nucléaire de Doel mais également en France où plusieurs centrales ont été survolées². Ces survols n'ont pas été revendiqués, mais doit-on craindre que les drones ne soient plus uniquement des armes pour lutter contre le terrorisme mais plutôt la prochaine arme du terrorisme ?

En ces temps de récession économique, l'Europe a besoin plus que jamais d'identifier et de soutenir des opportunités permettant de booster la compétitivité industrielle, de promouvoir l'entrepreneuriat et de créer des nouveaux *businesses* pour générer de la croissance et de l'emploi³. Enrôlés dans l'armée depuis plus de 20 ans, les drones diversifient leurs compétences aujourd'hui dans les secteurs les plus traditionnels mais aussi les plus inattendus⁴. Habilités à réaliser des missions plus longues ou plus dangereuses que celles réalisées avec un pilote à bord, les drones permettent de réduire l'exposition de la vie humaine. Ils ont des avantages économiques mais aussi environnementaux grâce à une consommation et une émission de CO2 réduites⁵. Des centaines d'applications civiles ont été identifiées et de nouvelles vont encore apparaître. Les drones ne vont pas seulement révolutionner l'industrie aéronautique, ils vont aussi générer de nouveaux services. Mais le potentiel

¹ AFP, « L'homme qui avait revendiqué l'attaque de Charlie Hebdo tué par drone », *La libre*, 7 mai 2015, <http://www.lalibre.be/actu/international/l-homme-qui-avait-revendique-l-attaque-de-charlie-hebdo-tue-par-un-drone-554bb7dd35704bb01c2e2022>.

² BELGA, « Un drone a survolé la centrale nucléaire de Doel », *La libre*, 20 décembre 2014, <http://www.lalibre.be/economie/actualite/un-drone-a-survole-la-centrale-nucleaire-de-doel-54958a3c3570e9972507022f>.

³ Conseil de l'Europe, Commission Staff working document

Towards a European strategy for the development of civil applications of Remotely Piloted Aircraft Systems (RPAS), 13438/12, Bruxelles, 6 septembre 2012, pp. 4 et 5.

⁴ C. VINCENT, *de drones d'engins, sans pilotes et sans limites, les echos*, <http://www.lesechos.fr/enjeux/business-stories/enjeu-du-mois/02148899682-de-drones-dengins-sans-pilote-et-sans-limites-1117327.php>.

⁵ Flying new way- a boost for european creativity and innovation, Commission européenne, http://ec.europa.eu/enterprise/flipbook/rpas/?goback=.gde_941207_member_238344699#/1/zoomed, p. 4.

de croissance ne peut être pleinement exploité que si un cadre juridique adéquat est établi, d'où l'importance d'identifier ce cadre et de l'évaluer⁶.

Dans les esprits, les drones peuvent soulever des questions de sécurité, éthique et philosophique. En effet, les drones interpellent car ils représentent un danger, tant pour la sécurité aérienne que par leur intervention comme arme de guerre. En outre, les drones suscitent des difficultés sur le plan éthique et moral vu qu'ils sont identifiés comme des machines volantes qui récoltent de vastes quantités de données. Finalement, les drones posent également des questions philosophiques dans la mesure où ils symbolisent l'effet panoptique imaginé par les frères Bentham, repris par le philosophe Michel Foucault pour en faire la pierre angulaire d'une société disciplinaire axé sur le contrôle sociale.

Dans ce travail nous aborderons les tensions créées par les drones civils au sein de notre système juridique, principalement au niveau du respect de la vie privée et des règles relatives au traitement des données. Nous ne traiterons pas des drones militaires, bien qu'étant les premiers du genre, ceux-ci soulèvent des questions de droit international et politiques qui ne rentrent pas dans le cadre de cette étude.

Afin d'examiner si une conciliation est possible entre la vie privée et les drones dans un premier temps, nous déterminerons les contours de la vie privée en analysant la législation applicable aux drones en matière de vie privée et de traitement des données, (Première partie). Nous examinerons ensuite les diverses capacités des drones (Deuxième partie). Finalement, nous terminerons par identifier les manques dans la législation et nous proposerons des pistes de réflexion afin d'améliorer le respect de la vie privée et mieux ajuster le système juridique aux drones (Troisième partie).

⁶ Communication de la Commission au Parlement européen et au Conseil, Une nouvelle ère de l'aviation. Ouvrir le marché de l'aviation à l'utilisation civil de systèmes d'aéronefs télépilotés, d'une manière sur et durable, COM (2014) 207 final, Bruxelles, 8 avril 2014, p. 4.

PARTIE I : LA VIE PRIVEE

Communément appelés drones, ces aéronefs qui sont pilotés à distance sont appelés dans le jargon technique RPAS, « *Remotely Piloted Aircraft Systems* ». Le vocable « drones » regroupe donc une réalité large d'aéronefs dont le pilote ne se trouve plus à bord mais au sol et le dirige grâce à un lien radio. Ceux-ci font partie de systèmes aériens sans pilotes UAS, « *Unmanned Aircraft Systems* » parmi lesquels figurent également les aéronefs qui peuvent être programmés pour voler de manière autonome. Pour des questions de facilité et de compréhension nous utiliserons dans cette étude le mot drone pour désigner les RPAS.⁷

Comme l'écrit Benjamin Docquir le droit à la vie privée est lié à l'évolution des sciences et des technologies. Pour lui d'une certaine façon, ce sont les technologies nouvelles qui sont à l'origine du droit à la vie privée. De l'apparition de la photographie au développement des médias audiovisuelles et des réseaux informatiques, la technologie enrichit et intensifie les moyens de communication et de traitement de l'information mais met aussi de plus en plus en jeu la vie privée. L'évolution des technologies rend donc nécessaire l'adaptation du cadre juridique de protection de la vie privée⁸. Ainsi l'apparition des drones, en tant que technologie nouvelle, va entraîner des risques nouveaux pour le droit à la vie privée.

Droit à l'intimité mais aussi droit à l'autonomie personnelle, la vie privée est une notion floue. Son contenu n'est pas susceptible d'une définition complète. L'individu exerce son droit à la vie privée par les choix qu'il pose. Le développement du droit international des droits de l'homme a donné une dimension juridique autonome au droit à la vie privée. Le droit à la vie privée fut d'abord reconnu à l'article 12 de la Déclaration universelle de droit de l'homme, ensuite à l'article 8 de la Convention européenne des droits de l'homme.⁹

⁷ Flying new way- a boost for european creativity and innovation, Commission européenne, http://ec.europa.eu/enterprise/flipbook/rpas/?goback=.gde_941207_member_238344699#/1/zoomed, p. 4.

⁸ B. DOCQUIR, *Le droit de la vie privée*, Bruxelles, Larcier, 2008, pp. 29

⁹ *Ibid.*, p. 30.

Dans cette première partie nous commencerons par évaluer l'étendue de la vie privée (Chapitre I). Ensuite nous analyserons toute législation qui est susceptible de s'appliquer aux drones civils (Chapitre II)

CHAPITRE I : L'ETENDUE DE LA VIE PRIVEE

Le droit à la vie privée recouvre certains droits protégés par l'article 8 de la Convention européenne des droits de l'homme tels que ; le respect de la vie privée individuelle (Section I), la vie familiale (Section II), le respect du domicile (Section III) et le respect de la correspondance (Section IV). Le droit à la vie privée recouvre aussi des informations à propos duquel l'individu doit pouvoir exercer une certaine maîtrise : les données à caractère personnel (Section V) et le droit à l'image de la personne (Section VI).¹⁰

Section I. La vie privée de l'individu

La vie privée « *implique que chacun puisse vivre à l'abri des regards, mais aussi qu'il puisse décider de manière autonome la façon de conduire sa vie et divulguer ou non des éléments de vie privée* ». ¹¹

Dans la vie privée de l'individu on retrouve l'intégrité physique et morale, le droit à l'identité, les nuisances environnementales, et finalement l'intimité et l'autonomie, qui sont deux prérogatives qui se renforcent mutuellement.¹²

Le droit à l'intimité de l'individu s'oppose aux investigations des autorités publiques, et aux intrusions des tiers, même si elles sont menées pour des motifs légitimes. Même s'il est légitime que l'Etat recherche et poursuive les infractions, les méthodes d'enquête et de poursuite doivent pouvoir coexister avec l'intimité des personnes recherchées et des citoyens.¹³ Le droit à l'autonomie se retrouve en particulier dans la protection des données à caractère personnel et dans le droit à l'image. Le droit à l'autonomie comporte aussi le droit à la libre disposition de son corps. Dans un

¹⁰ B. DOCQUIR, *op. cit.*, p. 65.

¹¹ *Ibid.*, p. 65.

¹² *Ibid.*, pp. 65 à 71.

¹³ *Ibid.*, p. 66.

arrêt¹⁴, la Cour de Strasbourg a reconnu le droit à la libre disposition de son corps comme un élément du droit à la vie privée.¹⁵

La vie privée individuelle est protégée aussi bien l'article 8 de la Convention européenne des droits de l'homme que par l'article 22 de la Constitution.

Section II. La vie familiale

Le concept de vie familiale utilisé par la Cour a évolué avec le temps, ce qui reflète ainsi l'attitude changeante de la société européenne. Pour la Cour, la vie de familiale ne se cantonne pas uniquement aux relations fondées par le mariage. Pour déterminer cette notion de « vie familiale », il peut être utile de prendre en compte d'autres éléments tels que la durée de la vie de couple, l'existence d'enfants au sein de la famille.¹⁶ Par cette arrêt¹⁷, la Cour a adopté une approche souple compte tenu de la diversité des formes de vie familiale. Dans la mesure où la Cour décide de l'existence d'une vie de famille au cas par cas, il n'est pas possible d'énumérer toutes les relations qui pourraient constituer une vie familiale.¹⁸ Ainsi, tous les liens de nature sociale, morale ou culturelle qui rassemblent des individus peuvent constituer la vie familiale¹⁹.

La vie familiale est garantie par l'article 8 de la Convention européenne des droits de l'homme, ainsi que par l'article 22 de la Constitution.

Section III. Le domicile

La notion de domicile ne se restreint pas à l'habitation privée, ni au lieu où la personne est inscrite au registre de la population. Le domicile s'étend plutôt à tout lieu où une personne mène sa vie privée, qu'il s'agisse d'une habitation propre ou louée, d'une chambre d'hôtel ou d'une caravane.²⁰ La Cour a défini le domicile dans

¹⁴ Cour eur. D.H., 29 avril 2002, *Pretty c. Royaume Uni*, Requête no 2346/02, [http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-65003#{"itemid":\["001-65003"\]}](http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-65003#{)

¹⁵ B. DOCQUIR, *op. cit.*, pp. 66 et 67

¹⁶ Cour eur. D.H., 22 avril 1997, Requête n° 21830/93, http://www.rtdh.eu/pdf/19970422_xyz_c_royaume-uni.pdf

¹⁷ Cour eur. D.H., 22 avril 1997, Requête n° 21830/93, http://www.rtdh.eu/pdf/19970422_xyz_c_royaume-uni.pdf

¹⁸ I. ROAGNA, « La protection du droit au respect de la vie privée et familiale par la Convention européenne des droits de l'homme », *Séries des précis droits de l'homme du Conseil de l'Europe*, Conseil de l'Europe Strasbourg 2012, pp. 31 et 32.

¹⁹ B. DOCQUIR, *op. cit.*, p. 72.

²⁰ *Ibid.*, p. 74.

plusieurs arrêts comme le lieu où une personne réside de façon permanente ou avec lequel elle a des liens suffisants et continus. La protection du domicile permet de protéger la personne contre toute intrusion de tiers ou des autorités publiques.²¹

L'article 15 de la constitution, en plus de l'article 8 de la Convention européenne des droits de l'homme préserve le domicile des individus. Les articles 148 et 439 du Code pénal punissent l'introduction non autorisée dans le domicile.

Section IV. Le respect de la correspondance

L'article 8 de la Convention européenne des droits de l'homme ne traite pas spécifiquement des communications mais parle de « correspondance ». Seulement cette notion de correspondance ne se limite pas aux lettres, elle s'étend, au contraire, à toutes les formes de communication, orales ou écrites, quelque soit le moyen de communication utilisé : téléphone fixe ou mobile, courriel électronique, ...²² De cette façon, enregistrer à distance des conversations en rue pourrait constituer une ingérence dans le droit au respect de la correspondance. Tant l'écoute que l'enregistrement des conversations peuvent porter atteinte au secret de la correspondance.²³

En plus de la protection de l'article 8 de la Convention européenne des droits de l'homme, la correspondance est protégée par l'article 29 de la Constitution belge.

Section V. Les données à caractère personnel

La loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*²⁴ poursuit les mêmes objectifs que la Directive 95/46/CE du Parlement européen et du Conseil, puisque cette loi fut modifiée pour transposer en droit belge les dispositions de la directive. Le but recherché par le législateur était de consolider la maîtrise de l'individu sur son « image informationnelle »²⁵. Pour ce motif, la loi reprend de la directive la définition

²¹ I. ROAGNA, *op. cit.*, p. 83

²² B. DOCQUIR, *op. cit.*, p. 76

²³ *Ibid.*, p. 77.

²⁴ Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993, modifié en dernier lieu par la loi du 18 mars 2014, *M.B.*, 28 mars 2014.

²⁵ B. DOCQUIR, *op. cit.*, p. 88.

la plus large possible de « données à caractère personnel ».²⁶ Ainsi, la loi définit ces données comme : « *toute information concernant une personne physique identifiée ou identifiable, désignée ci-après "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* »²⁷.

Les données à caractère personnel sont des informations qui méritent d'être protégées. Mais elles sont également nécessaires aux missions des pouvoirs publics et sont une source de contenu indispensable aux entreprises. Il convient donc de trouver un équilibre entre le pouvoir de traiter ces données et la nécessité de préserver la vie privée.²⁸

Section VI. Le droit à l'image

Il est certain que le visage et le corps d'un individu sont propres à la vie privée. Leur exposition publique est de nature à révéler à autrui des connaissances sur l'état, les activités, les opinions, les préférences de la personne et par conséquent sur une partie importante de sa vie privée²⁹. Dans un arrêt, la Cour de Strasbourg a reconnu que le droit à l'image entre dans le champ de la vie privée³⁰. Le droit à l'image peut être protégé par trois régimes juridiques distincts : (i) l'article 8 de la Convention européen des droits de l'homme, (ii) la réglementation sur le traitement des données à caractère personnel, et (iii) le droit à l'image tel qu'il en résulte de la jurisprudence et de la doctrine en matière de droit de la personnalité.³¹ Le droit à l'image développé par la jurisprudence sera exposé dans la dernière section consacré aux sources jurisprudentielles du Chapitre II.

²⁶ B. DOCQUIR, *op. cit.*, pp. 88 et 89.

²⁷ Article 1 de la Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993, modifié en dernier lieu par la loi du 18 mars 2014, *M.B.*, 28 mars 2014.

²⁸ B. DOCQUIR, *op. cit.*, pp. 86 et 87.

²⁹ *Ibid.*, p. 97.

³⁰ Cour eur. D.H., 24 juin 2004, *Von Hannover c. Allemagne*, [http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-66402#{\"itemid\":\[\"001-66402\"}](http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-66402#{\).

³¹ B. DOCQUIR, *op. cit.*, p. 97.

Comme le souligne Bernard Mouffe³², on pourrait représenter le droit à l'image et le droit à la vie privée comme deux cercles sécants. En effet, la vie privée comprend d'autres éléments que la seule image et il peut y avoir dans l'image d'autres éléments qui s'écartent de la vie privée. Néanmoins, ces deux concepts juridiques partagent une partie commune importante. La protection de la vie privée est mieux organisée que celle de du droit à l'image. Il est fréquent de voir que la juridiction saisie d'un contentieux qui vise une image attentatoire, sanctionne l'exploitation de l'image par le biais de l'article 22 de la Constitution ou l'article 8 de la Convention européenne des droits de l'homme.³³

Section VII. Qui sont les bénéficiaires de la protection de la vie privée ?

Si l'on prend la formulation de l'article 8 de la Convention européenne des droits de l'homme, on lit « *toute personne a droit au respect de sa vie privée et familiale* ». Le droit à la vie privée est attaché à la seule qualité d'être humain. Ce droit ne peut être soumis à la vérification d'aucune autre condition de droit ou de fait. Si l'on reprend l'article 1^{er} de cette même Convention, cette disposition stipule que tout pays contractant doit reconnaître à toute personne relevant de leur juridiction les droits reconnus par le titre premier de la Convention dont fait partie l'article 8. La Belgique doit donc protéger la vie privée des belges, des nationaux des autres Etats contractants, des ressortissants des Etats non parties et des apatrides.

CHAPITRE II : LES SOURCES DU DROIT A LA VIE PRIVEE

Dans un premier temps nous analyserons les sources internationales de la vie privée (Section I). Ensuite, nous verrons quels règles belges protègent ce droit (Section II). Finalement, nous terminerons par les sources jurisprudentielles de celui-ci (Section III).

Section I. Droit international

Au niveau international, on retrouve plusieurs textes qui consacrent le droit à la vie privée. Tout d'abord, il y a l'article 12 de la Déclaration universelle des droits

³² B. MOUFFE, *Le droit à l'image*, Waterloo, Kluwer, 2013, pp 90 et 91

³³ *Ibid.*, pp 90 et 91.

de l'homme qui stipule que : « *Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.* »

Ensuite, sur le plan européen, la vie privée est consacré par deux organisations : le Conseil de l'Europe et l'Union européenne. Le Conseil de l'Europe regroupe 47 pays qui tous ont adhéré à la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. La violation de cette Convention est sanctionnée par la Cour européenne des droits de l'homme à Strasbourg.³⁴ La Belgique, membre de l'Union Européenne est soumise aux traités fondateurs, au droit dérivé et à l'autorité de la Cour de justice à Luxembourg. Celle-ci, conjointement avec les juridictions nationales, assure le respect du droit à la vie privée.

A. Le droit du Conseil de l'Europe.

A1. La Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales

Adoptée le 4 novembre 1950 et rentrée en vigueur le 3 septembre 1953, l'article 8 cette Convention, mieux connu sous le nom de Convention européenne des droits de l'homme, stipule :

« 1. *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.*

2. *Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.* »

Comme le dit Benjamin Docquir, cette disposition constitue « *en même temps la pierre angulaire et le fil d'Ariane du droit à la vie privée* »³⁵. Le respect et l'interprétation de l'article 8 de la Convention relève de la compétence de la Cour

³⁴ B. DOCQUIR, *op. cit.*, pp. 36 et 37.

³⁵ *Ibid.*, p. 289.

européenne des droits de l'homme. Par l'existence de cette juridiction internationale condamnant les Etats qui violent la Convention, son article 8, tel qu'il est interprété par la Cour, a joué un rôle historique dans le développement et l'expansion du droit à la vie privée devant les cours et tribunaux des Etats parties à la Convention.³⁶ La Cour a ainsi été essentielle pour le développement de ce droit, en soulignant la nécessité pour elle d'interpréter les termes de la Convention de façon évolutive, jugeant que but de la Convention est d'assurer une protection du droit non pas théorique mais effective et concrète.³⁷

On reconnaît un effet direct aux traités internationaux protégeant la vie privée. Cet effet direct permet aux individus d'invoquer directement devant le juge belge le respect du droit fondamental à la vie privée. L'effet direct vertical, se retrouve à l'article 8 de la Convention européenne des droits de l'homme qui interdit l'ingérence de l'Etat dans la vie privée. Cet article impose par ailleurs des obligations positives dans le chef de l'Etat. L'effet direct horizontal, quant à lui, se retrouve à l'article 2 de la loi du 2 décembre 1992, qui confirme que l'obligation de respecter les droits et libertés, notamment le droit à la vie privée, s'impose à toute personne de droit privée et de droit public. Cette disposition légale consacre ainsi la thèse de l'applicabilité horizontale du droit à la vie privée à l'occasion d'un traitement de données.³⁸

A2. La Convention n°108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnelle

Cette Convention est adoptée le 28 janvier 1981 et est entrée en vigueur le 1^{er} octobre 1985. La Convention a pour but de garantir à toute personne, pour tout traitement automatisé des données personnelles, peu importe sa nationalité ou sa résidence, le respect des droits fondamentaux et notamment du droit à la vie privée.

³⁶ B. DOCQUIR, *op. cit.*, p. 37.

³⁷ *Ibid.*, p. 38.

³⁸ *Ibid.*, pp. 46 à 49.

A3. Recommandations et résolutions du Comité des ministres du Conseil de l'Europe

Dans le prolongement de la Convention 108, le comité des ministres établit des recommandations et des résolutions dans le cadre d'activités spécifiques des pouvoirs publics ou des entreprises. Certes, celles-ci ne sont pas contraignantes mais elles peuvent néanmoins servir de référence.³⁹

B. Le droit communautaire

B1. La charte des droits fondamentaux de l'Union européenne

Les droits fondamentaux furent d'abord l'œuvre d'une reconnaissance par la Cour de justice de l'Union. Ce n'est qu'en 2000 qu'ils furent entérinés de manière expresse par le législateur dans la *Charte des droits fondamentaux de l'Union européenne*. Dans le droit de l'Union, la protection des droits fondamentaux tendent vers une protection équivalente que celle offerte par la Convention européenne des droits de l'homme.⁴⁰

L'article 7 de la Charte des droits fondamentaux est presque identique à ce qu'on a à l'article 8 de la Convention européenne des droits de l'Homme :

« Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications. »

L'article 8 de la Charte traite de manière séparé du droit à la protection des données. Ceci confirme que les règles de protection des données ont une certaine autonomie et peuvent être condamnées indépendamment d'une atteinte à la vie privée. Le but de cette double approche est de défendre de façon concrète la double de la vie privée, c'est-à-dire de droit à l'intimité et de droit à l'autonomie (dont les données à caractère personnel sont une composante).⁴¹ L'article 8 de la Charte prévoit :

« 1. Toute personne a droit à la protection des données à caractère personnel la concernant.

2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime

³⁹ B. DOCQUIR, *op. cit.*, pp. 38 et 39.

⁴⁰ *Ibid.*, pp. 39 et 40.

⁴¹ *Ibid.*, p. 41.

prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante ».⁴²

B2. La directive 95/46/CE du Parlement européen et du Conseil relatives à la protection des données à caractère personnel

La directive, par sa nature, harmonise le droit de l'Union en ce qui concerne la protection des données. La Cour, dans l'affaire *Rechnungshof*⁴³, ajoute que les dispositions de la directive, en ce qu'elles règlent le traitement des données à caractère personnel, doivent être interprétées à la lumière des droits fondamentaux, qui font partie intégrante des principes généraux du droit dont la Cour assure le respect.⁴⁴

1. *Champ d'application*

Le champ d'application de la directive, assure une balance entre le respect de la vie privée et la libre circulation des données personnelles⁴⁵. L'article 3 paragraphe 1 stipule que la directive s'applique aux traitement de données à caractère personnel automatisé ou non. Le concept de traitement automatisé est *a priori* assez large pour que puisse être inclus les outils transportés par les drones pour la vidéosurveillance, des microphones et bien d'autres⁴⁶.

⁴² Art. 8 de la Charte des droits fondamentaux de l'Union européenne, *J.O.U.E.*, C.326, 26 octobre 2012.

⁴³ C.J.C.E., 20 mai 2003, *Rechnungshof* (C-465/00) contre Österreichischer Rundfunk et autres et Christa Neukomm (C-138/01) et Joseph Lauermann (C-139/01) contre Österreichischer Rundfunk, *Rec. C.J.C.E.*, p. I-04989, <http://curia.europa.eu/juris/document/document.jsf?docid=48330&doclang=FR>.

⁴⁴ C.J.C.E., 20 mai 2003, *Rechnungshof* (C-465/00) contre Österreichischer Rundfunk et autres et Christa Neukomm (C-138/01) et Joseph Lauermann (C-139/01) contre Österreichischer Rundfunk, *Rec. C.J.C.E.*, p. I-04989, <http://curia.europa.eu/juris/document/document.jsf?docid=48330&doclang=FR>.

⁴⁵ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, Study on privacy, data protection and ethical risks in civil Remotely Piloted Aircraft Systems operations, rapport finale, Bruxelles, Commission européenne, 2014 p. 68.

⁴⁶ *Ibid.*, p. 68.

Vu que la directive s'applique tant aux entités publiques qu'aux entreprises privées, certains preneurs d'information sont expressément exclus du champ de la directive.⁴⁷

i) *Les autorités de l'Etat*. Tout d'abord la directive ne s'applique pas aux traitements de données effectués par l'Etat dans le domaine du droit pénal et/ou dans le but de maintenir la sécurité publique, la défense, la sûreté de l'Etat. En effet, les traitements de données ayant pour objet la sécurité publique, la défense, la sûreté de l'Etat, la recherche et la poursuite des infractions sont une prérogative nationale, pour lesquels les Etats membres ont la compétence exclusive.⁴⁸

La directive n'est donc pas applicable aux traitements des données personnelles fait pas les forces de l'ordre lors de l'utilisation d'un drone. Les drones, opérés par les autorités étatiques, identifiant des personnes lors d'un événement en vue d'assurer sûreté publique, ne seront pas sujets aux dispositions de la directive. Toutefois, cela ne veut pas dire que ces autorités ne doivent pas tout mettre en œuvre pour se conformer aux exigences établies par la jurisprudence de l'article 8 CEDH et l'article 7 de la charte de droits fondamentaux.⁴⁹

ii) *Les activités exclusivement personnelles et domestiques*. Suivant l'article 3, paragraphe 2, la directive ne s'applique pas lorsque des données à caractère personnel sont traitées par des personnes physiques dans l'exercice d'activités exclusivement personnelles ou domestiques. Dans l'arrêt *Bodil Linqvist*⁵⁰, la Cour interprète cette exemption comme ne visant que les activités qui s'insèrent dans la vie privée et familiale du particulier. Le traitement ne sera plus domestique lorsque ce traitement est constitué de la publication sur internet car ces données deviennent accessibles à un

⁴⁷ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, p. 68.

⁴⁸ *Ibid.*, p. 69.

⁴⁹ Groupe de travail « Article 29 », Opinion 4/2004 on the processing of personal Data by means of Video Surveillance, 11750/02/EN, WP 89, Bruxelles, 11 février 2004, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp89_en.pdf, p.13.

⁵⁰ C.J.C.E., 6 novembre 2003, *Bodil Linqvist*, C-101/01, *Rev. C.J.C.E.*, p. I-12971 <http://curia.europa.eu/juris/document/document.jsf?text=&docid=48382&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=14633>.

nombre indéterminé de personnes.⁵¹ Ainsi, l'arrêt *Bodil Linqvist* enseigne que l'individu qui traite des données personnelles par l'utilisation d'un drone civil, et ensuite publie ou transmet ces données à un nombre indéfini de personnes ne sera pas dispensé des dispositions de la directive.⁵² On peut penser à l'exemple de la mise sur internet d'une vidéo prise par un drone.

Le Groupe de travail « Article 29 », dans une opinion de 2004⁵³, apporte des précisions sur l'interprétation de l'exemption de la directive en cas de vidéosurveillance faite à des fins personnelles ou domestique. L'exemption s'applique lorsque la vidéosurveillance concerne l'intérieure de la résidence pour la prévention du vol, ou en connexion avec la gestion de la famille. Une deuxième situation à laquelle l'exception s'applique est le cas de la vidéosurveillance installée à l'extérieur ou proche des lieux privés dans un but de protection de la propriété et/ou assurer la sécurité. Toutefois, la directive est moins claire quant au fait de déterminer si cette exception est prévue uniquement pour la famille individuelle. Si tel est le cas, alors lorsqu'un même système de surveillance est prévu par plusieurs propriétaires, l'exception à l'application de la directive ne devrait pas s'appliquer.⁵⁴ Dans le même sens, un drone utilisé par un individu pour surveiller sa propre propriété comprenant sa maison et les alentours de celle-ci, ne tombera pas sous le champ d'application de la directive. Le drone utilisé par un village ou une commune, pour surveiller plusieurs zones non sécurisées de ce village/commune, devra aussi respecter la directive.⁵⁵

iii) *Activités journalistiques et artistiques*. Lors de traitements des données à des fins de journalisme ou d'expression artistique, l'article 9 de la directive laisse aux législateurs nationaux le choix entre un régime d'exemptions ou d'exceptions afin de concilier le droit à la vie privée avec les règles régissant la liberté d'expression.⁵⁶

⁵¹ C.J.C.E., 6 novembre 2003, *Bodil Linqvist*, C-101/01, *Rev. C.J.C.E.*, p. I-12971, <http://curia.europa.eu/juris/document/document.jsf?text=&docid=48382&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=14633>.

⁵² R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, p. 69.

⁵³ Groupe de travail « Article 29 », Opinion 4/2004 on the processing of personal Data by means of Video Surveillance, 11750/02/EN, WP 89, Bruxelles, 11 février 2004, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp89_en.pdf, p. 14 et 15.

⁵⁴ Groupe de travail « Article 29 », Opinion 4/2004 on the processing of personal Data by means of Video Surveillance, 11750/02/EN, WP 89, Bruxelles, 11 février 2004, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp89_en.pdf, p. 14 et 15.

⁵⁵ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, p. 70.

⁵⁶ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, p. 70.

L'arrêt *Satamedia*⁵⁷ donne une interprétation large aux mots « aux seul fin du journalisme ». Il inclut dans la notion de « journalisme » la liberté d'expression qui comprend la liberté de recevoir et de communiquer des informations.⁵⁸

2. Le Groupe de travail « Article 29 »

Par ailleurs, la directive prévoit la création d'un groupe de protection des personnes à l'égard du traitement des données à caractère personnel, ci-après dénommé Groupe de travail « article 29 ». La mission de ce groupe est, d'une part, d'examiner les dispositions nationales prises par les Etats Membre en application de la directive et d'autre part, de conseiller et donner des avis à la commission.⁵⁹

3. Notion de « donnée à caractère personnel »

La notion de « donnée à caractère personnel » est plus complexe, elle est définie à l'article 2 de la directive comme : « *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* »⁶⁰. Bien qu'on puisse voir cette définition comme trop vague et pas assez pratique, le Groupe de travail « Article 29 » a publié une opinion sur cette notion pour assurer une compréhension commune. Suivant le Groupe, les données à caractère personnel doivent signifier toute information relative à une personne identifiée ou identifiable, une personne identifiable étant quelqu'un qui peut être identifié directement ou indirectement.⁶¹

⁵⁷ C.J.C.E., 16 décembre 2008, Tietosuoja-valtuutettu contre Satakunnan Markkinapörssi Oy et Satamedia Oy, C-73/07, Rev. C.J.C.E., p. I-09831, <http://curia.europa.eu/juris/document/document.jsf?docid=76075&doclang=FR>.

⁵⁸ C.J.C.E., 16 décembre 2008, Tietosuoja-valtuutettu contre Satakunnan Markkinapörssi Oy et Satamedia Oy, C-73/07, Rev. C.J.C.E., p. I-09831, <http://curia.europa.eu/juris/document/document.jsf?docid=76075&doclang=FR>.

⁵⁹ Art. 30 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, J.O.C.E., L.281, 23 novembre 1995.

⁶⁰ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, p. 68.

⁶¹ Groupe de travail « Article 29 », Opinion 4/2007 on the concept of personal data, 01248/07/EN WP 136, Bruxelles, 20 juin 2007, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.

Tout d'abord, le Groupe de travail explique que la directive s'applique aux images et aux sons collectés aux moyens de CCTV ou d'autres moyens de vidéosurveillance. Les données biométriques et de localisations sont aussi considérées comme des données à caractère personnel.⁶²

Le Groupe de travail rajoute que des images et un son correspondant à une personne identifiée ou identifiable constitue des données à caractère personnel : (i) même si elles ne sont pas associées avec les détails de la personne ; (ii) même si elles ne concernent pas des personnes dont le visage a été filmé ; (iii) quelque soit le média utilisé.⁶³

Par ces deux remarques, le Groupe de travail « Article 29 » prend en compte les futures technologies mais il veille aussi à délimiter aussi la notion large de « données à caractère personnel ». Par exemple, si un cliché pris par un drone ne montre que le dessus de la tête d'une personne et qu'on ne peut identifier celle-ci sans utiliser des techniques très poussées, ce cliché ne devrait pas être considéré comme contenant des données personnelles. Par contre, la même photo prise du jardin d'une maison et dont on peut facilement identifier le propriétaire, sera considérée comme des données à caractère personnel.⁶⁴

B3. Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) (2012/0011 (COD), 25.01.2012.)

La directive 95/46/CE fait actuellement l'objet d'un réexamen, et sera probablement remplacé par cette proposition de règlement. Ce règlement ne prévoit rien de spécifique en matière de drones mais certaines provisions du règlement peuvent être pertinentes pour répondre aux éventuelles préoccupations concernant le

⁶² Groupe de travail « Article 29 », Opinion 3/2012 on developments in biometric technologies, 00720/12/EN WP193, Bruxelles, 27 avril 2012, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf.

⁶³ Groupe de travail « Article 29 », Opinion 4/2007 on the concept of personal data, 01248/07/EN WP 136, Bruxelles, 20 juin 2007, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.

⁶⁴ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, pp. 68 et 69.

traitement des données à caractère personnel. Le règlement a en effet comme objectif de fournir des règles technologiquement neutres⁶⁵ La rapide évolution des technologies, mais aussi l'augmentation spectaculaire du partage et de la collecte de données, créent de nouveaux enjeux. Les nouvelles technologies ont augmenté les possibilités pour les entreprises comme pour les pouvoirs publics d'utiliser les données personnelles dans le cadre de leurs activités. La création d'un climat juridique de confiance est dès lors vital au développement économique.⁶⁶ Cette proposition de règlement sera plus détaillée dans la troisième partie de cette étude.

B4. Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale

Comme nous l'avons vu, la directive 95/46/CE ne s'applique pas aux traitements de données effectuées à des fins de sécurité et d'application de la loi. A l'inverse, cette décision-cadre s'applique aux traitements de données en relation avec la sécurité, spécialement exclus de la directive. Son inconvénient réside dans le fait que cette décision ne s'applique qu'aux échanges de données transfrontaliers.⁶⁷

B5. Proposition de directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ou d'exécution de sanctions pénales, et à la libre circulation de ces données

Cette proposition, tout comme la Décision-cadre s'applique aux activités répressives, mais à l'inverse de cette dernière, la proposition de directive s'applique aux traitements transfrontaliers mais aussi domestiques.

⁶⁵ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, p. 75.

⁶⁶ Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), 25 janvier 2012.

⁶⁷ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, p. 79.

B6. Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques)

Cette directive spécifie et complète la directive générale 95/46/CE, qui ne s'applique pas aux traitements de données effectuées à des fins de sécurité et d'application de la loi⁶⁸. On sait que les drones peuvent être utilisés pour les télécommunications en fournissant un système de communication et un service de réseau. Mais ces drones pourraient aussi intercepter les communications, et leur contenu, un outil qui pourrait s'avérer intéressant pour les forces de l'ordre.

Les articles 5, 6, et 9 de la directive de 2002 prévoient deux principes : la confidentialité et l'anonymisation. Les opérateurs doivent assurer la confidentialité des contenus des communications et des données, mais aussi anonymiser le transfert de données et les données de localisation.⁶⁹ L'article 15 prévoit cependant une exception à ces deux principes lors de la mise en œuvre d'une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique. Ces mesures peuvent être pris des mesures prises pour la surveillance, par un drone du gouvernement, des communications ou des données liées à ces communications, afin de (i) sauvegarder la sécurité nationale, (ii) assurer la défense et la sécurité publique, ou (iii) garantir la prévention ou la poursuite d'infractions pénales. Cette disposition fait également référence à l'article 13 de la directive 95/46/CE qui prévoit ces mêmes exceptions pour le responsable du traitement des données.⁷⁰ Enfin, l'interception de communications et de données, telles que du contenu ou des données de localisation, par un opérateur de drones civils, est prohibée, à moins que l'opérateur n'ait obtenu le consentement de l'utilisateur du système de communication.⁷¹

⁶⁸ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, p. 80.

⁶⁹ Art. 5, 6 et 9 de la Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), *J.O.C.E.*, L.201, 31 juillet 2002.

⁷⁰ Art. 15 de la Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), *J.O.C.E.*, L.201, 31 juillet 2002.

⁷¹ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, p. 81.

Bien que l'article 8 de la Convention européenne des droits de l'homme vise indéniablement les moyens de communication qu'offrent les nouvelles technologies, la spécificité des nouvelles technologies nécessitent l'adoption de règles propres à ce secteur. Ainsi, le Parlement européen et le Conseil ont adopté le 13 juillet 2002 la directive 2002/58. Cette directive « vie privée et communications électronique » fut transposée en droit belge par la loi du 13 juin 2005 relative aux communications électroniques. L'objectif de la directive est de cibler non seulement les télécommunications classiques, mais aussi les communications effectuées par voie électronique, notamment le courrier électronique, les SMS, les messageries instantanées, la téléphonie par internet, etc.⁷²

Section II. Droit belge

A. La Constitution belge

L'article 22 consacre le droit à la vie privée : « *Chacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi. La loi, le décret ou la règle visée à l'article 134 garantissent la protection de ce droit* ». ⁷³

L'article 29 consacre le secret des lettres : « *Le secret des lettres est inviolable. La loi détermine quels sont les agents responsables de la violation du secret des lettres confiées à la poste* ». ⁷⁴

Enfin l'article 15 est relatif à l'inviolabilité du domicile : « *Le domicile est inviolable; aucune visite domiciliaire ne peut avoir lieu que dans les cas prévus par la loi et dans la forme qu'elle prescrit* » ⁷⁵.

On remarque après lecture de ces trois articles un parallèle avec les quatre éléments visés par l'article 8 de la Convention européenne des droits de l'homme ; la

⁷² B. DOCQUIR, *op. cit.*, p. 79.

⁷³ Art. 22 de la Constitution belge.

⁷⁴ Art. 29 de la Constitution belge.

⁷⁵ Art. 15 de la Constitution belge.

vie privée et familiale, le domicile et la correspondance. Tout comme l'article 8 de la Convention, l'article 22 de la constitution permet à l'Etat de limiter ce droit à la vie privée.⁷⁶

B. La loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

La loi de 1992 doit être comprise à l'aide des droits fondamentaux et notamment l'article 8 de la Convention européenne des droits de l'homme. Tout traitement de données à caractère personnel doit respecter les trois conditions cumulatives de l'ingérence dans la vie privée : (i) être prévu par la loi (ii) être justifié par la poursuite d'un but légitime nécessaire dans une société démocratique, (iii) être proportionné. On identifie ces conditions dans les obligations pointues de la loi de 1992, et spécifiquement les articles 4 et 5 qui sont une reprise telle quelle des articles 6 et 7 de la directive 95/34/CE.⁷⁷

Dans cette partie nous analyserons d'abord le champ d'application de la loi, ensuite les conditions de traitement. Nous examinerons aussi la responsabilité. Finalement, nous verrons la protection des droits des individus.

B1. Champ d'application

1. *Ratione materiae.* la loi est destinée à prémunir les personnes contre le traitement abusif des données à caractère personnel. Elle détermine les droits de la personne dont les données sont traitées mais aussi les obligations qui pèsent sur le responsable du traitement des données pour qu'il respecte les conditions de l'ingérence dans la vie privée. La loi de 1992 institue la Commission de la protection de la vie privée (si après dénommé également « Commission vie privée »), chargée de vérifier que les données sont traitées dans le respect des droits de la personne concernée. Elle rend aussi des avis et des recommandations sur toute question relative à la protection de la vie privée dans la cadre de la loi du 8 décembre 1992, mais aussi dans le cadre d'autres lois qui protègent la vie privée à l'égard des traitements des

⁷⁶ B. DOCQUIR, *op. cit.*, pp. 43 et 44.

⁷⁷ *Ibid.*, p. 111.

données à caractère personnel, par exemple les articles de la Constitution.⁷⁸ La loi de 1992 a connu des modifications importantes, dont la première est la transposition en droit belge de la directive 95/34/CE. Une autre modification majeure est celle faite par le législateur belge pour changer la composition de la Commission vie privée vu les questions toujours plus précises auxquelles la Commission est confrontée.⁷⁹

2. *Ratione personae.* Seuls les opérateurs économiques, les journalistes et professions artistiques ainsi que les autorités étatiques rentrent dans le champ d'application de la loi. Les particuliers sont exemptés de la loi lors d'activités à des fins personnelles et domestiques, qui sont d'interprétation restrictive⁸⁰.

(i) *Les opérateurs économiques* : Les entreprises sont le premier destinataires de la loi. Ils sont soumis à l'entière de la loi.

(ii) *Journalistes et professions artistiques et littéraires* : Dans la même idée de balance des intérêts entre la liberté d'expression et la protection de la vie privée, les traitements effectués par les journalistes ou les professions artistiques ou littéraires bénéficient d'exceptions aux obligations qui pèsent sur le responsable des traitements de données.⁸¹ Ils devront toutefois toujours respecter les articles 4 et 5 de loi, qui impose un traitement loyal des données. Les données devront être collectés pour des finalités déterminées, exactes, et conservées pour une durée raisonnable.

(iii) *Les autorités de l'Etat* : La loi prévoit aussi des exceptions pour le traitement des données réalisé par la police judiciaire, la police administrative, la Sûreté de l'Etat, le Service renseignements, et la sécurité des forces armées.⁸² Tout comme les journalistes, les autorités de l'Etat doivent respecter les articles 4 et 5 de la loi.

⁷⁸ Art. 29 et 30 de la Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993, modifié en dernier lieu par la loi du 18 mars 2014, *M.B.*, 28 mars 2014.

⁷⁹ <http://www.privacycommission.be/fr/la-loi-vie-privee>.

⁸⁰ C.J.C.E., 6 novembre 2003, Bodil Linqvist, C-101/01, *Rev. C.J.C.E.*, p. I-12971
<http://curia.europa.eu/juris/document/document.jsf?text=&docid=48382&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=14633>.

⁸¹ Art. 3 de la Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993, modifié en dernier lieu par la loi du 18 mars 2014, *M.B.*, 28 mars 2014.

⁸² Art. 3 de la Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993, modifié en dernier lieu par la loi du 18 mars 2014, *M.B.*, 28 mars 2014.

B2. Les conditions du traitement de données

Trois conditions doivent être respectées par tout auteur d'un traitement de données, que le traitement soit fait par un opérateur économique, les autorités de l'Etat ou encore des journalistes.

1. La légalité du traitement de données

La loi prévoit de manière exhaustive les seuls cas dans lesquels le traitement de données est autorisé. Cependant, ces différents cas sont définis de façon large. Il n'est pas exact d'avancer qu'un traitement de données doit inévitablement être autorisé par l'intéressé.⁸³ L'article 5 de la loi, qui est une reprise de l'article 7 de la directive, prévoit que le traitement de données ne peut être effectué que dans les situations où : (i) la personne a donné son consentement (article 5 point a) (ii) le traitement est nécessaire à l'exécution d'un contrat dont la personne concernée par le traitement est partie (article 5 point b); (iii) il permet le respect d'une obligation qui pèse sur la personne concernée par le traitement (article 5 point c); (iv) il permet la sauvegarde de l'intérêt vital de la personne concernée (article 5 point d); (v) le traitement est indispensable à la réalisation d'une mission d'intérêt public, ou une mission relevant de l'autorité publique dont est investi le responsable du traitement ou le destinataire des données relevées (article 5 point e); et (vi) le traitement sert à la réalisation d'un intérêt légitime poursuivi par le responsable du traitement ou le destinataire des données collectées (article 5 point f).⁸⁴ Il est important de noter que ce 6^e cas repris par le législateur peut être regrettable dans la mesure où il peut entraîner des confusions avec la seconde condition pour l'ingérence : la légitimité.

Pour comprendre la portée de cet article, notons que la notion de « traitement » est très vaste et couvre toute opération relative à des données à caractère personnel. En pratique, on observera que l'article 5 de la loi révèle qu'il n'est pas autorisé d'utiliser des données à caractère personnel, sauf si le traitement envisagé repose sur une base légale expresse.⁸⁵

⁸³ B. DOCQUIR, *op. cit.*, p. 111.

⁸⁴ Art. 5 de la Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993, modifié en dernier lieu par la loi du 18 mars 2014, *M.B.*, 28 mars 2014.

⁸⁵ B. DOCQUIR, *op. cit.*, p. 112.

Le traitement de données dans le cas du consentement de la personne. Il faut souligner que le consentement est une manifestation de la volonté qui peut être expresse ou implicite. Ce consentement doit être libre, c'est-à-dire dépourvu de toute pression extérieure. Il doit aussi être spécifique et viser précisément un ou des traitements bien déterminés, effectué par un responsable identifié et pour des finalités explicites. Finalement, ce consentement devra être informé, la personne concernée devra disposer de toutes les informations indispensables en rapport avec le traitement des données.⁸⁶ Dans une opinion, le Groupe de travail « Article 29 » précise que le consentement devra être séparé et en connexion avec les activités de surveillance du lieux où la personne mène sa vie privée⁸⁷. Même si souvent le consentement est essentiel pour que les activités de surveillance soient effectuées légalement, il existe un débat sur le poids à accorder au consentement. En effet, l'exigence de consentement s'estompe quelque peu dans les autres cas repris à l'article 5 de la loi, où il n'est pas nécessaire. Les incertitudes qui entourent le consentement sont renforcées du fait que la surveillance ou la vidéosurveillance peuvent être entrepris sans l'exigence d'un consentement explicite, car dans ces situations le consentement est présumé par le simple fait qu'un individu entre dans un lieu public.⁸⁸

Néanmoins, dans la plupart des cas, les organismes commerciaux opérant avec des drones auront besoin soit du consentement explicite de l'individu sujet du traitement, soit d'une autre base légale pour la surveillance, tel qu'un arrangement contractuel.⁸⁹

2. *Légitimité dans le traitement des données*

L'article 4, §1^{er}, 2° de la loi de 1992 précise que les données doivent être collectées pour des finalités qui doivent être déterminées, explicites et légitimes. Cet article 4 précise que ces données ne peuvent pas être ensuite traitées de manière incompatible avec ces finalités.

⁸⁶ B. DOCQUIR, *op. cit.*, pp. 113 et 114.

⁸⁷ Groupe de travail « Article 29 », opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance, 11750/02/EN WP 89, Bruxelles, 11 février 2004, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp89_en.pdf.

⁸⁸ M. L., GRAS « The Legal Regulation of CCTV in Europe », *Surveillance and Society Review*, Vol. 2 No. 3, 2004, [http://www.surveillance-and-society.org/articles2\(2\)/regulation.pdf](http://www.surveillance-and-society.org/articles2(2)/regulation.pdf)

⁸⁹ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, p. 72.

« Ce principe de légitimité est la clé de voûte du régime de protection prévu »⁹⁰ par la loi du 8 décembre 1992. Une ou plusieurs finalités précises devront être choisies par le responsable du traitement et ce dès le début du processus. Des finalités exprimées de manières trop générales correspondent à une absence de finalité, et des finalités trop restreintes rendent impossible l'utilisation postérieure des données en raison de la règle de compatibilité. Le responsable exprime ces finalités en de termes clairs, complets, et précis. De la sorte, la personne concernée par les traitements pourra comprendre quel sera l'utilisation faite de ses données. Finalement, fonder le traitement sur une base légale au sens de l'article 5 de la loi ne constitue pas une fin légitime *de facto*, dans le respect l'article 4, §1^{er}, 2^o.⁹¹

3. La proportionnalité du traitement des données

Il faut un juste équilibre entre les droits de la personne concernée par le traitement et ceux de la personne responsable du traitement. Les données récoltées devront être pertinentes au regard de la finalité du traitement. Ce ne sera qu'à cette condition que le traitement pourra être jugé nécessaire au but poursuivi, comme le prescrit l'article 8, §2 de la Convention européenne des droits de l'homme. On le verra la loi du 8 décembre 1992 contient des règles plus précises afin d'assurer cette proportionnalité.⁹²

Il faut vérifier si (i) les moyens mis en place par le responsable sont raisonnable par rapport aux buts poursuivis, (ii) le contenu des données est conforme et proportionné à ces buts, et (iii) qu'il n'existe pas de moyens utilisant moins de données ou des données moins intrusives pour obtenir le même objectif.⁹³

En plus de ces trois conditions, la loi impose également que le traitement des données soit loyal et licite (l'article 4, §1^{er}, 1^o). Le principe de loyauté équivaut à un devoir général d'information et de transparence envers la personne concernée par le traitement des données.⁹⁴ En outre, l'article 4 contient aussi le principe de conformité

⁹⁰ B. DOCQUIR, *op. cit.*, p. 122.

⁹¹ *Ibid.*, pp. 122 et 124.

⁹² *Ibid.*, p. 131.

⁹³ *Ibid.*, p. 132.

⁹⁴ *Ibid.*, p. 132.

et d'exactitude des données exigeant que les données soient adéquates, pertinentes, mises à jour mais aussi non excessive au regard des finalités pour lesquelles elles sont collectées. Finalement, les données devront être conservées pour une durée nécessaire par rapport aux finalités poursuivies et sous une forme qui autorise l'identification de la personne concernée.⁹⁵

B3. Responsabilité du traitement

En droit belge la responsabilité lié au traitement des données incombe à toute personne ayant traité les données. La notion de traitement recouvre toute opération relative à des données à caractère personnel⁹⁶. Le responsable du traitement a supporte l'obligation de préciser la base légale du traitement (la légalité) et la charge de prouver l'intérêt légitime poursuivi (la légitimité). Si le responsable des données fait reposer le traitement sur le 6^e cas de l'article 5, f) (la réalisation d'un intérêt légitime), il devra établir, sous le contrôle du juge, que l'équilibre entre les intérêts est respecté. Il faudra donc évaluer le caractère intrusif du traitement et voir si d'autres moyens disponibles peuvent mener à un résultat similaire. En effet le responsable doit opter la voix la moins dommageable.⁹⁷

B4. Protection des droits de la personnes dont les données sont traitées

La personne concernée par le traitement de données bénéficie de droits.

- (i) *Droit à l'information.* Basé sur le principe de transparence, la personne concernée doit être informée que des données la concernant sont traitées, mais aussi de la finalité de ce traitement, de la catégorie de données dont il s'agit et ses destinataires auxquels ces données sont communiquées.⁹⁸ (Transposition des articles 10 et 11 de la directive)
- (ii) *Droit d'accès et de rectification.* L'article 9 de la loi du 8 décembre 1992 octroie à la personne concernée par le traitement un droit d'accès aux données et de rectification pour la personne concernée par les traitements.

⁹⁵ Art. 4 de la Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993, modifié en dernier lieu par la loi du 18 mars 2014, *M.B.*, 28 mars 2014.

⁹⁶ B. DOCQUIR, *op. cit.*, p. 112.

⁹⁷ *Ibid.*, pp. 116 et 117.

⁹⁸ Art. 9 de la Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993, modifié en dernier lieu par la loi du 18 mars 2014, *M.B.*, 28 mars 2014.

- (iii) *Droit d'opposition.* L'article 12 de la loi, reconnaît un droit d'opposition à la personne concernée qui lui permet de s'opposer à tout moment, pour des raisons prépondérantes et légitimes, à ce que les données la concernant ne fassent plus l'objet d'un traitement, sauf lorsque la licéité du traitement est basé sur l'article 5, b) et c). En cas d'opposition justifié, le traitement mis en œuvre par le responsable ne peut plus porter sur ces données.⁹⁹ (Transposition de l'article 14 de la directive).
- (iv) *Droit de réparation.* Si le responsable du traitement viole la loi de 1992, l'article 39 de celle-ci prévoit que toute personne ayant subi un dommage du fait d'un traitement illicite a le droit d'obtenir réparation du préjudice subi auprès du responsable du traitement.¹⁰⁰ (Transposition de l'article 23 de la directive).

B5. Comparaison avec la directive 95/46/CE

On constate que la loi belge est plus stricte que la directive. Malgré qu'elle prévoit comme la directive une exemption totale pour les particuliers, elle ne prévoit que des certaines exceptions pour les autorités étatiques, alors que la directive prévoit pour ceux-ci une exemption totale. Pour les journalistes et les professions artistiques et littéraires, sur base du choix laissé par la directive, le législateur belge a opté pour des exceptions plutôt qu'un régime d'exceptions.

C. La loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance.

Les drones sont fort utiles aux autorités chargées de la surveillance afin de prévenir et poursuivre les infractions mais ils pourraient également être utilisés par les particuliers pour surveiller leur domicile.¹⁰¹ Puisqu'un drone équipé avec une caméra pourrait être inclus dans la définition de caméra mobile expliquée ci-dessous, cette loi du 21 mars 2007 entre dans le cadre juridique régissant les drones.

⁹⁹ Art. 12 de la Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993, modifié en dernier lieu par la loi du 18 mars 2014, *M.B.*, 28 mars 2014.

¹⁰⁰ Art. 39 de la Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993, modifié en dernier lieu par la loi du 18 mars 2014, *M.B.*, 28 mars 2014.

¹⁰¹ L'utilité des drones est développée dans la seconde partie de cette étude.

C1. la surveillance en général.

En général, toute surveillance par l'Etat doit respecter les prescrits du Code pénal et les lois particulières. En matière de vie privée, outre la loi du 8 décembre 1992, la surveillance devra respecter l'article 8 de la Convention européenne des droits de l'homme qui protège contre l'ingérence des autorités de l'Etat.¹⁰² Celles-ci sont ne justifiées que pour des besoins clairement identifiables puisque le Code pénal et les lois particulières définissent précisément les comportement infractionnels, les modes d'investigation qui peuvent être mis en œuvre, ainsi que les limites à respecter¹⁰³.

Dans la mesure où la Belgique dispose d'une législation propre à la vidéosurveillance, il est pertinent d'étudier cette loi qui, à l'inverse de la loi du 8 décembre 1992, est applicable tant aux particuliers qu'aux autorités de l'Etat.

C2. La vidéosurveillance

L'objectif de la loi du 21 mars 2007 est de prévenir, constater et déceler les infractions contre les biens et les personnes. Il s'agit d'une *lex specialis* qui complète la loi du 8 décembre 1992. Ainsi sort du champ d'application de la loi de 2007 l'utilisation générale de caméras à d'autres fins que la prévention, le constat et le décèlement d'infractions pour lesquelles seule la loi de 1992 s'applique.

1. Définition

La vidéosurveillance peut être définie comme « *une surveillance à distance des lieux publics ou privés, à l'aide de caméras qui transmettent les images saisies à un équipement de contrôle qui les reproduit sur des écrans* »¹⁰⁴. Dans le monde anglo-saxon, le terme CCTV est utilisé et signifie Closed Circuit Television¹⁰⁵.

2. Analyse de la législation spécifique à la vidéosurveillance.

Cette loi du 21 mars 2007 est applicable à tout système de vidéosurveillance qu'il soit géré par les pouvoirs publics ou par des personnes privées. La loi s'applique

¹⁰² B. DOCQUIR, *op. cit.*, p. 291.

¹⁰³ *Ibid.*, p. 292.

¹⁰⁴ G. L. BOURDOUX, Vidéosurveillance et police : quel(s) profit(s) pour la police ? Quel(s) coût(s) pour la société ?, dans La vidéosurveillance. Entre usages politiques et pratiques policières, sous la direction de M-S. DEVRESSE et J. PIERET, avec la collaboration de P. BELLIS et L. NOLET, p. 9

¹⁰⁵ G. L. BOURDOUX, *op. cit.*, p. 9.

à tout *système d'observation fixe ou mobile*. Par « mobile » la loi vise une caméra de surveillance qui est déplacée au cours de l'observation afin de filmer à partir de différents lieux ou positions¹⁰⁶.

L'article 8 de la loi de 2007 prévoit que les caméras de surveillance cachées sont interdites. Est considérée comme « cachée » une caméra filmant une personne n'ayant pas donné son autorisation. Par contre, pénétrer dans un lieu où il y a un pictogramme annonçant une caméra vaut autorisation. La présence dans un lieu ouvert ou dans un lieu fermé accessible au public, dans lequel les caméras de surveillance mobiles sont utilisées de manière visible, est également considérée comme une autorisation. Les caméras de surveillance mobiles, montées à bord de véhicules, de navires ou d'aéronefs non banalisés, sont réputées être utilisées de manière visible.¹⁰⁷

La loi du 6 janvier 2003 sur les méthodes particulières de recherche et quelques autres méthodes d'enquête, exclut l'application de la loi de 2007. Toutefois, la Commission de la vie privée ainsi que la Commission permanente de la police locale et de la police fédérale sont d'avis que la loi de 2007 sur les caméras est applicable à l'utilisation de caméras de surveillance par les services de police dans leur mission de police administrative ou de police judiciaire lorsque ces missions n'entrent pas dans les conditions prévues par la loi de 2003.¹⁰⁸

3. *Caméras mobiles*

Puisque dans ce travail nous nous intéressons aux drones, nous ne verrons que les règles spécifiques aux caméras mobiles. Ainsi, suivant l'article 7/1 de la loi de 2007, la police peut recourir aux caméras mobiles dans le cadre de la surveillance de grands rassemblements. Les caméras sont utilisées dans des lieux ouverts ou fermés mais accessibles au public et pour des missions non permanentes et dont la durée

¹⁰⁶ Art. 2 de la Loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, *M.B.*, 31 mai 2007, modifié en dernier lieu par la loi du 4 avril 2014, *M.B.*, 25 avril 2014.

¹⁰⁷ Art. 8 de la Loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, *M.B.*, 31 mai 2007, modifié en dernier lieu par la loi du 4 avril 2014, *M.B.*, 25 avril 2014.

¹⁰⁸ C. ATAS et M. DEGROOVER, La pratique de la vidéosurveillance en Belgique : application et évaluation de la loi du 21 mars 2007, in dans La vidéosurveillance. Entre usages politiques et pratiques policières, sous la direction de M-S. DEVRESSE ET J. PIERET, avec la collaboration de P. BELLIS et L. NOLET, Bruxelles, Politeia, p. 79 et 80.

d'exécution est limitée.¹⁰⁹ Selon nous, il serait bénéfique d'étendre le champ d'application à d'autres types de surveillance que les rassemblements, tels que l'observation, ou les contrôles visuels, mais aussi à l'usage dans des lieux fermés. Ces lieux sont définis à l'article 2 de la loi de 2007 . Puisque la loi s'applique également aux particuliers, il est malheureux de ne pas avoir prévu l'utilisation de ces caméras mobiles à d'autres fins et pour des lieux fermés non accessibles au public. Les particuliers aurait pu utiliser les drones comme mode de surveillance de leur propriété, afin de déceler, prévenir ou constater des infractions, comme le vol ou le vandalisme par exemple.¹¹⁰

4. *L'installation de caméras mobiles*

Suivant l'article 7/2 de la loi de 2007, l'installation de caméras mobiles dans un lieu ouvert doit être prise par l'officier de police administrative responsable. Ce dernier en informe le bourgmestre concerné dans les plus brefs délais. La décision de recourir à des caméras de surveillance dans un lieu fermé accessible au public, quant à elle, est prise par le bourgmestre. La responsabilité opérationnelle est assurée par l'officier de police administrative qui pourra en cas d'extrême urgence décider seul du recours aux caméras. Il en informe cependant le bourgmestre immédiatement. Lorsque l'officier de police prend la décision de recourir aux caméras mobiles, il notifie sa décision à la Commission de la vie privée.

5. *L'utilisation de caméras mobiles*

L'officier de police est chargé de veiller à ce que l'utilisation des caméras soit ciblée, efficace, et qu'elle respecte les prescrits de la loi du 8 décembre 1992. Le visionnage des images en temps réel par la police n'est autorisé que dans le but de permettre aux services d'agir préventivement ou immédiatement en cas d'infraction, de dommage, de nuisance, ou d'atteinte à l'ordre public.

6. *Enregistrement des images filmées*

L'enregistrement est autorisée: (i) pour prendre des mesures préventives destinées à éviter les perturbations ; (ii) pour rassembler des preuves de faits

¹⁰⁹ Art. 7/1 de la Loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, *M.B.*, 31 mai 2007, modifié en dernier lieu par la loi du 4 avril 2014, *M.B.*, 25 avril 2014.

¹¹⁰ B. DOCQUIR, *op. cit.*, p. 318.

constitutifs d'infractions, de dommages ou de nuisances ; (iii) pour la recherche ou l'identification de personnes, suspects, victimes, et témoins. Si ces images ne servent pas à accomplir les objectifs visés aux points (ii) et (iii), elles ne peuvent être conservées plus d'un mois.¹¹¹

7. *Les images interdites*

Les caméras ne pourront cependant pas fournir d'images qui portent atteinte à l'intimité de la personne. Elles ne pourront pas non plus servir à recueillir des informations relatives aux opinions philosophiques, religieuses, politiques, ou syndicales, à l'origine ethnique ou sociale, à la vie sexuelle, ou à l'état de santé des personnes concernées.¹¹²

8. *Conservation et preuve*

Bien que la loi traite de la conservation des images à la fin de l'article 7/2 de la loi de 2007, elle reste muette quant à l'utilisation d'images comme preuve en justice. La doctrine est cependant d'avis que les images obtenues en violation de la loi de 2007 ne sont pas sanctionnées par la nullité des preuves. Il reviendra au juge d'apprécier la recevabilité de celles-ci, en appréciant leur fiabilité et leur éventuelle violation du procès équitable.¹¹³

D. *La loi du 13 juin 2005 relatives aux communications électroniques.*

Cette loi est la transposition de la directive vie privée et communication électronique¹¹⁴, ainsi que la directive 2006/24/CE sur la conservation de données générées ou traitées dans les communications.¹¹⁵ La loi prévoit la confidentialité des

¹¹¹ Art. 7/2 de la Loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, *M.B.*, 31 mai 2007, modifié en dernier lieu par la loi du 4 avril 2014, *M.B.*, 25 avril 2014.

¹¹² Art. 10 de la Loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, *M.B.*, 31 mai 2007, modifié en dernier lieu par la loi du 4 avril 2014, *M.B.*, 25 avril 2014.

¹¹³ B. DOCQUIR, *op. cit.*, p. 302.

¹¹⁴ Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), *J.O.C.E.*, L.201, 31 juillet 2002.

¹¹⁵ Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, *J.O.U.E.*, L.105, 13 avril 2006.

communications et du contenu des communications. Conformément au principe de « neutralité technologique » que sous-tend la directive 2002/58, ce régime est applicable à toutes formes de communication¹¹⁶.

L'article 124 de la loi du 13 juin 2005 transpose l'article 5 de la directive. Il pose que, sauf en cas d'autorisation donnée par les personnes directement ou indirectement concernées par une communication électronique, personne ne peut (i) prendre connaissance du contenu de la communication ni des données techniques y afférentes, (ii) identifier les personnes concernées par la transmission de l'information et son contenu, ou encore (iii) modifier, supprimer, révéler, stocker, ou faire un usage quelconque du contenu, des données techniques ou de l'identification ainsi obtenue. Cette protection est en partie similaire à la protection issue de l'article 314*bis* du Code pénal, mais elle s'étend aux données de trafic et de localisation et elle porte sur l'existence même d'une information transmise par voie de communication, par opposition au seul contenu visé par l'article 314*bis* du Code pénal.¹¹⁷

E. Articles 47sexies et 47septies du Code de procédure pénal.

Ces articles encadrent la surveillance systématique, prérogatives de la police.

Section III. La jurisprudence

L'image étant un attribut de la vie privée. Elle constitue une donnée à caractère personnel pour laquelle on peut appliquer la loi sur le traitement des données du 8 décembre 1992. Nonobstant le fait qu'une exemption générale existe pour les particuliers, et des exceptions pour les journalistes et les autorités de l'Etat, on peut concevoir d'appliquer à ceux-ci le droit à l'image en temps que construction jurisprudentielle, détaillée ici.¹¹⁸

¹¹⁶ B. DOCQUIR, *op. cit.*, p. 79.

¹¹⁷ B. DOCQUIR, *op. cit.*, pp. 79 à 81.

¹¹⁸ *Ibid.*, p. 137.

A. Nature et contenu du droit à l'image

Le droit à l'image est un droit subjectif, reconnu à chaque individu, de nature extrapatrimoniale dans la mesure où il s'insère dans les droits de la personnalité. Cependant, vu qu'il devient courant de rentabiliser son image, ce droit peut également avoir une composante patrimoniale.¹¹⁹

A1. Définition

En Belgique comme en France, chaque individu possède un droit exclusif sur son image. Toute personne peut s'opposer à l'exposition, la diffusion, l'utilisation et l'exploitation de son image sans son consentement, qu'importe le support, le mode de diffusion et la bonne ou mauvaise foi du diffuseur.¹²⁰ Même si notre système juridique ne contient pas de définition légale, la jurisprudence et la doctrine définissent depuis longtemps le droit à l'image, comme étant le droit exclusif d'une personne d'autoriser, ou pas, la reproduction ou la représentation de son image afin de protéger sa personnalité¹²¹.

Même si plusieurs dispositions dont référence le droit à l'image, il reste une création jurisprudentielle.¹²² Le droit à l'image est souvent influencé par la jurisprudence française. Contrairement à la Belgique, la France a édicté un certain nombre d'infractions pénales qui protègent le droit à l'image.¹²³ L'article 226-1 du Code pénal français prévoit que porte atteinte à la vie privée d'autrui, le fait de fixer, enregistrer ou transmettre, sans le consentement, l'image d'une personne en lieu privé.

A2. Le droit à l'image est un droit subjectif

Le droit à l'image est un droit subjectif qui repose sur les règles de la responsabilité civile¹²⁴, les droits de la personnalité et plus spécialement sur la protection de la vie privée.¹²⁵ La Cour de justice de l'Union souligne, dans *Reklos et*

¹¹⁹ M. ISGOUR, *Le droit à l'image*, Bruxelles, Larcier, 2014, p. 92 ; Civ. Bruxelles, 7 juin 1974, *J.T.*, 1975, obs. M De Salle, p.136.

¹²⁰ B. MOUFFE, *op. cit.*, p. 5.

¹²¹ B. DOCQUIR, *op. cit.*, p. 98.

¹²² Bruxelles, 26 décembre 1888, *Pas.*, 1889, II, p. 94.

¹²³ B. MOUFFE, *op. cit.*, p. 6.

¹²⁴ X. DIJON, *Le sujet de droit en son corps*, Société d'études morales, sociales et juridiques, 1982, Namur, p. 178.

¹²⁵ B. MOUFFE, *op. cit.*, p. 6.

*Davourlis*¹²⁶, que l'image d'un individu, est un des attributs principaux de la personnalité d'un individu du fait qu'elle dégage son originalité. La Cour précise que la simple prise d'une photographie par autrui, indépendamment de sa publication ou diffusion, porte atteinte au droit à la vie privée¹²⁷.

Pour garantir au mieux la protection de ce droit subjectif, tant la doctrine que la jurisprudence¹²⁸ ont rapidement soutenu que le seul fait de porter atteinte à l'image constituait une faute.¹²⁹ Ainsi, toute atteinte au droit à l'image doit être sanctionnée et réparée sans que la victime ne doive apporter la preuve de la faute, ni celle de son dommage ou encore du lien causal, pour qu'il y ait une infraction au droit à l'image.¹³⁰ et ¹³¹. L'atteinte à l'image en elle-même entraîne la faute et le préjudice, peu importe le comportement ou la bonne ou mauvaise foi de l'auteur de cette atteinte¹³².

B. La personne est reconnaissable

La personne physique représentée sur l'image est le titulaire du droit à l'image, puisque c'est à elle que revient le contrôle de son image. Le droit à l'image porte sur la représentation des traits de son titulaire et protège ces traits physiques, notamment le visage mais aussi la silhouette ou tout autre élément corporel, à la condition qu'ils soient attribuables à une personne identifiée ou identifiable. En effet, l'introduction d'une demande au respect de son image est soumise à la condition que la représentation soit suffisamment individualisée et que la personne soit reconnaissable.¹³³ Il revient au tribunal de trancher si, du point de vue des tiers, la personne est reconnaissable sur l'image incriminée.¹³⁴ Une personne identifiable, mais présente sur le cliché que de manière accessoire ou accidentelle ou sur un cliché flou et de format réduit¹³⁵, ne sera pas jugée comme identifiable. De la même manière, une personne identifiable, mais qui se trouve mêlée au milieu d'autres,

¹²⁶ Cour eur. D.H., *Reklos et Davourlis c. Grèce*, 15 janvier 2009, req. n° 1234/05.

¹²⁷ I. Roagna, *op. cit.*, p. 21.

¹²⁸ Civ. Paris, 6 janvier 1976, *J.T.*, 1976, p. 209 ; Civ. Bruxelles, 7 juin 1974, *J.T.*, 1975, p. 135.

¹²⁹ J. MILQUET, « La responsabilité aquilienne de la presse », *Ann. Dr.*, 1989, p. 48.

¹³⁰ Trib. gr. inst. Paris, 24 septembre 1976, *J.C.P.*, 1977, IV, p. 256.

¹³¹ Civ. Gand (16^e ch.), 24 juin 2002, *A.M.*, 2002/3, p. 143, obs. M. Isgour.

¹³² B. MOUFFE, *op. cit.*, p. 9 ; M. ISGOUR, *op. cit.*, p. 68.

¹³³ B. MOUFFE, *op. cit.*, p. 23 ; B. DOCQUIR, *op. cit.*, p. 100.

¹³⁴ B. DOCQUIR, *op. cit.*, p. 99.

¹³⁵ Paris, 27 février 1974, *D.*, 1974, jur., p. 530, obs. R. LINDON, dans B. MOUFFE, p. 28.

risque de ne pas être considérée comme reconnaissable parce que l'attention d'un spectateur normal n'est pas attirée directement sur elle.¹³⁶

Dans certaines situations l'anonymisation d'une personne peut être exigée : (i) par la loi ; (ii) souhaitée par la personne ; ou (iii) faite de manière autonome par les médias pour préserver les droits et intérêts de la personne, notamment dans le cas où la presse n'a pas pu s'assurer du consentement explicite de la personne représentée.¹³⁷ La Cour, dans l'arrêt *Peck*¹³⁸, conclut à une atteinte à la vie privée, sur base de la violation de l'article 8 de la Convention européenne des droits de l'homme. Dans cet arrêt, les autorités publiques avaient communiqué les images d'une tentative de suicide d'une personne à la presse. Une caméra de surveillance installée sur la voie publique avait filmé les faits. La Cour a conclu en la violation de la vie privée, non pas pour l'enregistrement, mais du fait de la diffusion publique par les médias de ces images, constituant en la médiatisation de la personne, qu'elle ne pouvait pas prévoir compte tenu de ses attentes légitimes.¹³⁹

C. Le consentement exprès

L'affaire de l'hôtesse Sabena enseigne que toute diffusion de l'image d'une personne, en dehors du droit à l'information, ne peut se faire qu'avec son consentement exprès¹⁴⁰. Dans cette exigence, on retrouve des similitudes avec le consentement exigé de la personne pour le traitement de ses données, devant être libre, spéciale, et informé. Toute utilisation de l'image d'une personne à laquelle elle n'a pas valablement consenti sera illicite.¹⁴¹ La validité du consentement est régie par les règles du droit civil relatives à la formation de tout contrat (l'article 1108 et

¹³⁶ B. MOUFFE, *op. cit.*, p. 28.

¹³⁷ B. MOUFFE, *op. cit.*, p. 33.

¹³⁸ Cour eur. D.H., 28 janvier 2003, *Peck c. Royaume-Uni*, requête n° 44647/98, [http://hudoc.echr.coe.int/sites/eng-press/pages/search.aspx?i=003-688210-695728#{"itemid":\["003-688210-695728"\]}](http://hudoc.echr.coe.int/sites/eng-press/pages/search.aspx?i=003-688210-695728#{).

¹³⁹ Cour eur. D.H., 28 janvier 2003, *Peck c. Royaume-Uni*, requête n° 44647/98, [http://hudoc.echr.coe.int/sites/eng-press/pages/search.aspx?i=003-688210-695728#{"itemid":\["003-688210-695728"\]}](http://hudoc.echr.coe.int/sites/eng-press/pages/search.aspx?i=003-688210-695728#{).

¹⁴⁰ Bruxelles, 7 avril 2000, *J.T.*, 2001, p. 779.

¹⁴¹ Gand 1^{er} ch., 21 février 2008, *A.M.*, 2008/4, p. 318 ; B. DOCQUIR, *op. cit.*, p. 140.

suivant du Code civil relatif au consentement).¹⁴² Ce consentement doit être exprès c'est-à-dire que le consentement doit être certain et spécial : (i) certain car il doit être éclairé et ne pas laisser de doutes, et il ne pourra pas découler d'une tolérance¹⁴³ ou d'une complaisance antérieure¹⁴⁴ ; et (ii) spécial car il doit être donné spécifiquement pour des exploitations identifiées. Par exemple le fait qu'une personne accepte d'être photographié ne signifie pas qu'elle permet que ses traits soient exposés publiquement¹⁴⁵, ou le fait qu'une personne accepte la prise et la diffusion publique de son image ne signifie pas qu'elle admette qu'on en fasse des affiches de pub.¹⁴⁶ Tout élément de son image, concédé par la personne représentée, doit faire l'objet d'une interprétation stricte¹⁴⁷ et restrictive¹⁴⁸. Tout dépassement sera sanctionné¹⁴⁹. La charge de la preuve de l'obtention du consentement repose sur celui qui publie l'image¹⁵⁰.

Les caméras cachées ne peuvent être utilisées qu'exceptionnellement dans un intérêt majeur d'information. Le recours à ces caméras qui recueillent des images et des sons à l'insu des personnes doit être limité aux nécessités de l'actualité ou de l'information du public. L'anonymat des personnes doit être assuré afin que l'usage de ce procédé n'enfreigne pas le droit à l'image.¹⁵¹

D. Limites au droit à l'image

Vivre à l'abri des regards d'autrui est une des dimensions les plus fondamentales du droit à la vie privée. Cependant, la nécessité pour chacun de vivre en société est inévitable de sorte que le droit à la vie privée ne peut pas être un droit

¹⁴² B. MOUFFE, *op. cit.*, p. 35.

¹⁴³ Civ. Bruxelles, 17 janvier 1975, *J.T.*, 1975, p. 441.

¹⁴⁴ C. DOUTRELEPONT, « l'introuvable droit à l'image », in Mélanges offerts à Raymond Vander Elst, Tome I, Nemesis, p. 238, dans B. MOUFFE, *op. cit.*, p. 36.

¹⁴⁵ Bruxelles 2^e ch., 7 avril 2000, *J.T.*, 2001, p. 779 ; Gand, 20 septembre 2006, *Juristenkrant*, 2006, n°139, p. 5, obs. D. VOORHOOF.

¹⁴⁶ B. MOUFFE, *op. cit.*, p. 37.

¹⁴⁷ Bruxelles, 14 mai 1968, *J.T.*, 1968, p. 454 ; Civ. Liège, 24 septembre 1982, *J.L.M.B.*, 1982, p. 419.

¹⁴⁸ B. DOCQUIR, *op. cit.*, p. 141 ; Civ. Anvers, 12 juin 2008, *A.M.*, 2008, p. 321 ; Gand, 20 septembre 2006, *Juristenkrant*, 2006, n°139, p. 5, obs. D. VOORHOOF.

¹⁴⁹ Gand, 20 septembre 2006, *Juristenkrant*, 2006, n°139, p. 5, obs. D. VOORHOOF.

¹⁵⁰ B. MOUFFE, *op. cit.*, p. 42.

¹⁵¹ B. MOUFFE, *op. cit.*, pp. 70 et 71.

absolu.¹⁵² Comme le souligne G. Del Vecchion, l'individu doit tolérer une communication raisonnable et équitable de son image, lorsque la communication ne porte pas atteinte à l'essence même de sa personne, mais confirme l'existence de l'individu dans sa nature sociale. Pour Vecchion, une prohibition totale de toute représentation visuelle et graphique d'un individu ne serait imaginable que si celui-ci désire vivre dans un état de solitude totale. Or participer à diverses relations de la vie sociale implique déjà un consentement à ces communications et aux expositions de sa personne, qui sont la conséquence naturelle et logique de la vie sociale.¹⁵³ L'individu, par son choix de vivre en société, accepte donc de renoncer en partie à son image pour des raisons légitimes telles que la surveillance par les autorités par exemple.

Le droit à l'image n'est donc pas absolu. Des exceptions existent pour rééquilibrer des conflits entre plusieurs droits. Ainsi, selon le sujet de l'image, les conditions d'utilisation, le contexte dans lequel se trouve utilisé l'image, et les éventuelles droits à la liberté artistique ou d'information, un équilibre devra être trouvé.¹⁵⁴

Plusieurs exceptions au droit à l'image visent à équilibrer le droit à l'image et le droit à l'information. Ces exceptions ne nécessitent pas une autorisation de la personne représentée et ainsi permettent une utilisation raisonnable et non excessive de l'image. Ces exceptions sont les suivantes: (i) les personnes publiques car elles donnent une autorisation tacite à la reproduction de leur image ; (ii) l'image qui constitue une illustration dans un quotidien représentant une information légitime ; (iii) une personne étant mêlée à une information que la société est en droit de recevoir, ou contribuant à un débat d'intérêt générale¹⁵⁵ ; (iv) une personne participant à un événement d'actualité ; (v) la présence d'une personne sur un lieu public, qui regroupent les lieux du domaine public qui sont accessibles à tout le monde, sans restrictions ; (vi) le comportement de la personne, par exemple si elle publie des

¹⁵² B. DOCQUIR, *op. cit.*, p. 289.

¹⁵³ G. DEL VECCHIO, « Essai sur les principes généraux du droit », *Rev. crit. législ. jurisp.*, 1925, p. 185.

¹⁵⁴ B. MOUFFE, *op. cit.*, p. 105.

¹⁵⁵ Cour eur. D.H., 7 février 2012, *Von Hannover c. Allemagne (n°2)*, Requêtes nos 40660/08 et 60641/08, §109, [http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-109027#{"itemid":\["001-109027"\]](http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-109027#{); Cour eur. D.H., 7 février 2012, *Springer AG c. Allemagne*, Requête no 39954/08, §90, [http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-109035#{"itemid":\["001-109035"\]](http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-109035#{); Cour eur. D.H., 9 novembre 2006, *Leempoel et SA éd. Ciné-Revue c. Belgique*, Requête no 64772/01, §68, [http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-77921#{"itemid":\["001-77921"\]](http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-77921#{).

images sur son blog ou sur une page internet : et (vii) les images infractionnelles en raison de leur intérêt pour l'ordre public.¹⁵⁶

Conclusion sur le droit à l'image jurisprudentiel

Le droit à l'image développé par la jurisprudence peut aider à combler les lacunes découlant des exceptions prévues par la loi du 8 décembre 1992. En effet, ce droit permet de protéger les personnes contre les drones utilisés à des fins de voyeurisme par les particuliers. Il permet aussi de protéger la sphère privée des personnes contre les autorités étatiques, si aucun autre intérêt sociétal n'est supérieur. Finalement, ce droit préserve également la vie privée des individus contre les abus de la presse. Le droit à l'image réaffirme ainsi l'importance de la balance entre différents intérêts en présence.

¹⁵⁶ Pour plus d'information voir B. MOUFFE, *op. cit.*, pp. 129 à 165.

PARTIE II : LES CAPACITES DES DRONES

Bien que les drones soient une technologie moderne, leur développement remonte à la fin du 19^e siècle où des dirigeables remplis à l'hydrogène, contrôlés par des signaux radios qui émettaient des étincelles, volaient dans les salles de théâtres et de music-halls pour amuser la galerie. Durant la deuxième guerre mondiale les efforts pour créer une bombe volante ont produit le premier vol sans pilote. Pendant les 75 années suivantes les drones sont restés majoritairement une prérogative de la défense, qui continua à développer cette technologie pour le guidage de missiles, les tirs ciblés, et la surveillance. Les amateurs animés par la vieille envie de l'homme de pouvoir voler, ont également contribué à l'amélioration de la technologie. Récemment, l'idée que les drones puissent remplir toutes les tâches accomplies par les aéronefs équipés de pilotes prit de l'importance avec l'intervention de NATO au Kosovo, où des aéronefs sans pilotes ont été utilisés pour la surveillance en temps réelle et l'acquisition d'objectifs¹⁵⁷. Aujourd'hui il y a des centaines de modèles de drones et des milliers d'entreprises engagées dans leur design, leur conception, et leur utilisation.¹⁵⁸

Le développement récent des drones doit autant au développement informatique, qu'à l'imagerie numérique, qu'à la capacité de transférer des données ainsi qu'aux avancées dans la technologie aéronautique. La transmission de vidéos en direct est devenue une fonction standard des drones volant hors de vue, permettant ainsi aux pilotes et aux contrôleurs de voler en utilisant le FPV (*first person view*) de l'image transmise en temps réelle à une base au sol. De nombreux modèles de drones transportent du matériel additionnel : (i) de surveillance ; (ii) fournissant aux exploitants des images aériennes ; (iii) permettant des analyses géo spatiales et d'autres types de données. Grâce à leurs multiples capacités les drones peuvent soulever autant de questions de vie privée ou de traitements de données mêmes lorsqu'ils sont utilisés par des particuliers à des fins autres que la surveillance.¹⁵⁹

¹⁵⁷ European Advisory Group on Aerospace, « STAR 21: Strategic Aerospace Review for the 21st Century », Brussels, 2002.

¹⁵⁸ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit*, p. 173.

¹⁵⁹ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit*, pp. 173 et 174.

Dans cette deuxième partie nous allons examiner les différents types de drones civils utilisés et leurs capacités multiples et variées. Nous analyserons l'utilisation qu'il est fait des drones, leur équipement et le contexte dans lequel ils sont sollicités. Notre analyse sera orientée en partant des exploitants susceptibles d'utiliser les drones. Nous commencerons par les opérateurs commerciaux (Chapitre I), ensuite nous verrons l'utilité des drones pour les forces de l'ordre et les autorités étatiques (Chapitre II). Les journalistes et les cinéastes recourent également à l'usage des drones dans leur métier (Chapitre III). Ensuite nous analyserons l'utilité des drones pour les fournisseurs des télécommunications (Chapitre IV) et finalement nous traiterons de l'utilisation des drones par les particuliers (Chapitre V).¹⁶⁰

CHAPITRE I : LES OPERATEURS COMMERCIAUX

Les opérateurs économiques jouent un rôle moteur dans l'acceptation de l'utilisation des drones civils. Ils estiment que la prolifération des drones peut représenter un bénéfice non seulement financier, mais aussi au niveau de l'emploi, et en termes d'essor économique.¹⁶¹

Section I. Inspection d'infrastructures

L'inspection d'infrastructure est une des activités les plus populaires des drones civils. Le but premier est d'inspecter des objets. On retrouve l'utilisation des drones notamment dans la surveillance de pipe-lines, de sites nucléaires ou industriels et dans l'inspection des tours de téléphones mobiles, de ponts, d'éoliennes. De nombreux éléments permettent de penser que des domaines comme la raffinerie pétrolière, les usines chimiques, les centrales nucléaires, les centrales électriques, les barrages, pipe-lines, et l'énergie renouvelable seront un jour amenés à solliciter l'usage des drones.¹⁶² En effet, beaucoup de ces infrastructures sont difficiles d'accès ou sont situées dans des zones rurales. L'inspection et la surveillance de ces sites commencent par le domaine visuel. L'information est enregistrée par des caméras haute résolution qui permettent de filmer et de prendre des photos précises. Ces caméras haute résolution permettent, par exemple d'agrandir par après les images sur

¹⁶⁰ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, pp. 173 et 174.

¹⁶¹ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, p.174.

¹⁶² A. SNIDER, « Drones fly into nascent civilian market ripe with energy, environmental applications », *E&E Publishing*, 25 février 2012.

des zones spécifiques de l'objet observé ou de comparer différentes images. Ces inspections peuvent aussi être réalisées à l'aide d'images thermiques, spécialement conçues pour identifier des « hot spots », le long de lignes haute-tension et leurs stations de relais.¹⁶³

Section II. Autres services visuels

Les drones équipés de matériel photographique, avec des caméras à haute définition, peuvent aussi servir dans la capture d'images pour la vente ou l'utilisation à des fins publicitaires. Tout comme l'inspection d'infrastructures, dans cette utilisation il est souvent inévitable que ces prises d'images pour la vente ou la publicité incluent la présence de personnes dans l'image.¹⁶⁴

Section III. Usage à fin de cartographie

Les drones sont capables d'observer et de collecter de l'information sur des vastes zones. L'altitude à laquelle les drones volent et les caméras haute définition qui les équipent, sont particulièrement utiles pour la cartographie. Leur mobilité est aussi un grand avantage comparé aux satellites en orbite qui peuvent obtenir des images très détaillées mais pas sur une base continue. Certains de ces drones volant à haute altitude peuvent être munis aussi bien d'une caméra de jour que d'une caméra infrarouge, ou encore d'un radar à synthèse d'ouverture capable de fournir des images à travers les nuages, la pluie, le brouillard, de jour comme de nuit. La puissance des drones est telle que même les plus petits, comme les drones lancés à la main, sont capables de couvrir de larges étendus. Les drones peuvent également être équipés d'appareil photo fournissant des images 3D plus rapidement et à prix moins élevé que la traditionnelle technologie de laser LIDAR (*laser detection and ranging*).¹⁶⁵

Cet usage cartographique de drones peut aussi servir dans la construction, l'industrie minière, ou la surveillance géographique. Un drone peut aider à tracer une nouvelle route ou aménager un nouveau quartier résidentiel. Un recours aux drones peut également servir l'industrie du pétrole, du gaz ou de l'exploitation minière

¹⁶³ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, p. 174.

¹⁶⁴ *Ibid.*, p. 176.

¹⁶⁵ *Ibid.*, pp. 176 et 177.

nécessitant une reconnaissance aérienne et un arpentage géographique. Dans le cadre de catastrophes naturelles telles que séismes, des glissements de terrain, des inondations, ou des désastres causés par l'homme tels que de fuites de pétrole, les drones permettent aux autorités et aux secouristes d'identifier les zones affectées et d'évaluer l'ampleur des dégâts et les mesures à prendre.¹⁶⁶

Section IV. Observation de la terre

L'observation de la terre et la télédétection, aujourd'hui réalisées à l'aide de satellites ou d'avions conventionnelles, pourront être améliorées par la disponibilité et le faible coût qu'impliquent les drones. Des données utilisées pour l'observation du changement climatique, de la pollution atmosphérique, ou encore des analyses environnementales pourront être recueillies par des drones.¹⁶⁷ Des organisations environnementales et des gouvernements utilisent déjà des drones pour protéger des zones vertes, pour tracer et localiser la faune et prévenir l'érosion du sol.¹⁶⁸ Similairement, l'archéologie, la géologie, la métrologie, l'océanographie, et la sismologie, pourraient bénéficier toutes d'un apport des drones.¹⁶⁹

Les drones peuvent être équipés de capteurs biologiques, capables de détecter dans l'atmosphère la présence de microorganismes. Ils peuvent aussi être munis de capteurs chimiques utilisant la spectroscopie laser pour analyser la concentration d'éléments atmosphériques. Les drones ont l'avantage de pouvoir accéder à des zones dangereuses ou difficiles d'accès pour l'humain.¹⁷⁰ Par exemple, au Japon, des drones sont sollicités à la centrale nucléaire de Fukushima pour éviter que les équipes de chercheurs ne soient exposées à des taux dangereux de radiations.¹⁷¹

On pourrait même envisager que, dans le futur, les drones puissent manipuler l'environnement. En Chine, par exemple, une entreprise teste un « smog cleaning

¹⁶⁶ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit*, p. 177.

¹⁶⁷ *Ibid.*, p. 178.

¹⁶⁸ AUVSI, « The Benefits of Unmanned Aircraft Systems : Saving Time, Saving Money, Saving Lives », *Association for Unmanned Vehicle Systems International (AUVSI)*, p. 2, <https://epic.org/events/UAS-Uses-Saving-Time-Saving-Money-Saving-Lives.pdf>.

¹⁶⁹ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit*, p. 178.

¹⁷⁰ *Ibid.*, p. 178.

¹⁷¹ Pour plus d'exemple <http://increasinghumanpotential.org/cnet-uass-newest-mission-disaster-relief/>.

drone » pour essayer de lutter contre le problème chronique de pollution dans ce pays.¹⁷²

Section V. Agriculture

Les drones peuvent trouver un usage utile dans l'agriculture, la sylviculture, et dans la gestion de la pêche. La surveillance des champs par des caméras haute résolution peut contribuer à identifier des espèces invasives, des problèmes de sécheresse, et d'autres maladies. Cette surveillance est rapide et efficace. Dans ce cadre, les drones peuvent même être utilisés pour disperser du fertilisant, des pesticides et des fongicides.¹⁷³ En outre, de nombreux appareils installés sur les drones peuvent assister l'agriculture. Il y a l'indentification visuelle mais le drone peut également être équipé de capteurs thermiques ou d'imagerie hyper spectrale.¹⁷⁴

Section VI. Utilisations nouvelles

Une des forces des drones est leur polyvalence. Celle-ci permet aux drones de générer de nouveaux services et de développer de nouvelles industries.¹⁷⁵ Les équipements pouvant être montés sur les drones vont permettre de l'essor de nouveaux services. Par exemple, la volonté de la société *Amazon* de délivrer des produits aux consommateurs par drones.

Cependant, par ces diverses capacités et applications, il est fréquent que l'utilisation des drones implique la collecte de données par les opérateurs commerciaux. Il est donc essentiel que les opérateurs respectent les législations en la matière.¹⁷⁶

CHAPITRE II : LES FORCES DE L'ORDRE ET LES AUTORITES ETATIQUES

Les forces de l'ordre et les autorités de l'Etat sont des utilisateurs établis de drones. Ce sont aussi les utilisateurs les plus controversés. En outre, ils sont exemptés

¹⁷² M. BADKAR, "China May Use Drones To Kill The Smog Problem", *Business Insider*, 5 mars 2014, <http://www.businessinsider.com/china-is-testing-smog-clearing-drones-2014-3>.

¹⁷³ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit*, p. 179.

¹⁷⁴ *Ibid.*, p. 180 et 181; Pour plus d'information voyons <http://farmingdrones.com>.

¹⁷⁵ European RPAS Steering Group, *Roadmap for the intergation of civil Remotely-Piloted Aircraft Systems into the European Aviation System*, juin 2013.

¹⁷⁶ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit*, pp. 180 et 181.

de plusieurs législations sur la vie privée ou sur le traitement des données, auxquelles les opérateurs commerciaux doivent adhérer. Malgré cette exemption, l'opinion publique manifeste des attentes légitimes par rapport à la protection de la vie privée et de leurs données par ces utilisateurs. La prise en compte de ces attentes est notamment importante pour favoriser une réaction positive du public à l'égard des drones.¹⁷⁷

Section I. La surveillance de personnes

L'utilisation de drones par la police et à des fins répressives a provoqué de vastes critiques et des inquiétudes auprès des organisations non gouvernementales. Bien que l'utilisation de drones pour le maintien de l'ordre public est toujours controversée, ceux-ci ont été testés dans le cadre de plusieurs missions telles que : (i) la surveillance de foules lors de festivals, manifestations, ou événements sportifs ; (ii) la prévention de comportements antisociaux ; (iii) la détection de cultures de marijuana ; ou (iv) l'assistance de la police dans des poursuites et autres opérations.¹⁷⁸

Dans le cadre de missions de police, les drones servent entre autre à prendre des photos de la scène de crime, à rechercher et sauver des victimes, à l'investigation d'incendies criminelles, ou encore à la sûreté maritime. En effet, les drones permettent d'accomplir des missions, notamment de surveillance, semblables aux missions confiées aux hélicoptères de police, mais à un coût bien plus faible.¹⁷⁹

Pour contribuer à leurs missions « judiciaires », les drones peuvent être équipés de matériels multiples qui justifient le recours aux drones et les rendent incontournables. Citons les caméras à haute définition, les capacités GPS pour l'observation et la surveillance de foules ou de personnes, les caméras d'imagerie thermique pour la détection de plantation de marijuana¹⁸⁰, les microphones ou même des systèmes acoustiques complexes comportant un sonar passif pour la détection de bruits.¹⁸¹

¹⁷⁷ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, p. 181.

¹⁷⁸ *Ibid.*, pp. 181 et 182.

¹⁷⁹ *Ibid.*, p. 182.

¹⁸⁰ *Ibid.*, p. 182.

¹⁸¹ Adams technology Pvt. Ltd., "Battlefield Acoustics-Microflown", *Adams Technology*, <http://www.adams-tech.net/project/battlefield-acoustic-systems-microflown/>.

En plus de ces équipements, les drones pourraient être munis d'un logiciel pour observer les comportements humains et ainsi prévenir des comportements antisociaux, des intrusions dans des zones protégées, ou tout autre comportement à problèmes. Des logiciels intelligents « smart surveillance »¹⁸² permettent la détection de comportements douteux et anormaux par le profilage et l'exploitation des données. Cette technologie est spécialement utilisée pour la sécurité des frontières, l'antiterrorisme et la lutte contre la criminalité organisée.¹⁸³ Elle a permis de limiter le nombre de données collectées en utilisant des gâchettes et des filtres qui bloquent certaines données ou transmettent des images limitées.¹⁸⁴ Une entreprise japonaise « Secom » commercialise déjà un drone qui s'envole lorsqu'il y a une effraction et a la capacité de filmer les événements et même de suivre des sujets mobiles avec un capteur laser.¹⁸⁵ Une autre technologie qui peut équiper le drone est un mécanisme de reconnaissance faciale.

Section II. Protection civile

La protection civile comprend la planification et l'intervention en cas d'urgence et l'observation d'infrastructures critiques. Ceci concerne des acteurs publics mais aussi privés qui sont susceptibles d'utiliser des drones. Ils peuvent être utilisés pour observer et évaluer les dommages, pour apporter du matériel ou pour détecter des risques. L'aide humanitaire et les pompiers utilisent déjà les drones pour constater l'étendue et la propagation du feu et pour dresser une carte des environs contaminés par des matières ou des substances dangereuses.¹⁸⁶

Section III. Application de la loi

Les autorités de l'état peuvent utiliser les drones pour veiller à l'application de la loi ou d'une réglementation spécifique à certains secteurs. Cela peut comprendre la

¹⁸² R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, pp. 182 et 183.

¹⁸³ D. WRIGHT, M. FRIEDEWALD, S. GUTWIRTH, M. LANGHEINRICH, E. MORDINI, R. BELLANOVA, P. DE HERT, K. WHADWA ET D. BIGO, « Sorting out smart surveillance », *Computer Law & Security Review*, Vol. 26, 2010, pp. 10 et 11, trouvé sur http://works.bepress.com/serge_gutwirth/69/

¹⁸⁴ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, p. 183.

¹⁸⁵ J. FINGAS, « Secom offers a privacy drones, serves as our eyes when we're away », *Engadget*, 27 décembre 2012, <http://www.engadget.com/2012/12/27/secom-offers-a-private-security-drone/>.

¹⁸⁶ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, p. 184.

surveillance par drones de l'air, de la terre et de l'eau pour la pollution, le déboisement illégale, ou toute autre activité prohibée. En plus des autorités de l'Etat, les drones sont utilisés dans ce but par des gardes forestiers, des autorités de protection de l'environnement et des conseils locaux.¹⁸⁷

CHAPITRE III : LE JOURNALISME ET LE CINEMA

Comme pour les autorités étatiques, le journalisme et le cinéma bénéficient d'une exemption prévue par l'article 3, § 3 de la loi du 8 décembre 1992.¹⁸⁸ Les journalistes et cinéastes utilisent des caméras à haute résolution pour produire des images aériennes. L'exemption a été initialement prévue pour protéger la liberté d'expression et la liberté de la presse. Toutefois, il faut reconnaître que cette exemption est aussi susceptible d'entraîner des pratiques irresponsables.¹⁸⁹

CHAPITRE IV : LES FOURNISSEURS DE TELECOMMUNICATIONS

L'intérêt des drones dans le secteur des télécommunications a pris de l'importance suite à l'annonce de Facebook de leurs pourparlers avancés avec Titan Aerospace, producteur de drones solaires.¹⁹⁰

Les drones peuvent être utilisés comme satellites intermédiaires pour transporter des systèmes de communication et fournir des services à haut débit. Les modèles « Solara 50 » et « Solara 60 » de Titan Aerospace, peuvent être lancés de nuit et fonctionner sur batterie. Ensuite quand le soleil se lève, le drone de Titan Aerospace peut emmagasiner suffisamment d'énergie pour monter à 20 kilomètres au-dessus du niveau de la mer d'où ils peuvent rester cinq ans sans avoir besoin de se ravitailler.

Les drones peuvent encore être utilisés comme relais de communication. Un drone Solara peut produire une couverture pour un rayon d'environ 30 kilomètres

¹⁸⁷ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit*, p. 185.

¹⁸⁸ M. ISGOUR, *op. cit.*, p. 42.

¹⁸⁹ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit*, pp. 186 et 187.

¹⁹⁰ S. PEREZ ET J. CONSTINE, Facebook « Looking Into Buying Drone Maker Titan Aerospace », *Techcrunch.com*, 3 mars 2014, <http://techcrunch.com/2014/03/03/facebook-in-talks-to-acquire-drone-maker-titan-aerospace/>.

avec la possibilité de créer un réseau de communication continu.¹⁹¹ Facebook et Google prévoient de fournir l'accès à Internet par l'intermédiaire de drones à des personnes qui n'ont actuellement pas accès. Cette technologie permet de fournir des services de télécommunication haut débit à un coût bien moindre que ceux des satellites.¹⁹²

En plus de pouvoir fournir un service de télécommunication, les drones peuvent aussi être munis d'équipements qui permettent d'intercepter les télécommunications. Les données pouvant être recueillies sont des données de localisation, le contenu des communications et des informations personnellement identifiables.¹⁹³

CHAPITRE V : L'UTILISATION DE DRONES PAR LES PARTICULIERS

Actuellement plus de drones sont utilisés par les particuliers que par les forces de l'ordre. Grâce à la révolution des Smartphones et la rapide avancée de l'électronique accessible au grand public, les particuliers ont tous les éléments en main pour créer leur propre drone, et les utiliser à des fins privées ou domestiques. Les particuliers bénéficient d'exemption aussi, ce qui signifie que la majeure partie des utilisateurs de drones n'est pas couverte par les législations sur le traitement de données et sur la vie privée.¹⁹⁴

La majorité de ces drones est équipée avec des caméras à haute définition, telles que la GoPro. Les données sont principalement recueillies sous forme visuelle ou auditive. Ces drones sont souvent utilisés par des amateurs de photos ou de vidéos. Ces prises peuvent contenir de la photographie de paysages ou la réalisation de scènes.¹⁹⁵

¹⁹¹ S. GALLAGHER, « Almost orbital, solar-powered drone offered as “atmospheric satellite” », *Ars Technica*, 18 août 2013, <http://arstechnica.com/information-technology/2013/08/almost-orbital-solar-powered-drone-offered-as-atmospheric-satellite/>.

¹⁹² R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, p. 188.

¹⁹³ *Ibid.*, p. 188.

¹⁹⁴ *Ibid.*, p. 189.

¹⁹⁵ *Ibid.*, p. 189.

PARTIE 3 : INTERACTIONS ENTRE LA VIE PRIVEE ET LES DRONES, LA PROTECTION EST ELLE SUFFISANTE ?

Nous venons d'identifier les différents usages civils des drones ainsi que d'exposer les législations qui sont susceptibles de s'y appliquer. Mais sont-elles suffisantes? Pour chaque type d'utilisateurs de drones civils nous verrons quels problèmes ceux-ci posent en matière de vie privée, quelles lois leur sont applicables et nous identifierons ensuite les carences de ces législations (Chapitre I). Nous examinerons aussi les progrès envisagés dans la proposition de règlement européen (Chapitre II). Nous analyserons, par après, les mesures prises à l'égard des drones dans d'autres systèmes juridiques : la France et les Etats-Unis (Chapitre III). Finalement, nous explorerons des améliorations qui pourraient être apportées au cadre juridique applicable aux drones en Belgique (Chapitre IV).

CHAPITRE I : MENACES, LEGISLATIONS ET CARENCE

Nous pouvons diviser les utilisateurs de drones civils en quatre catégories ; les opérateurs commerciaux qui regroupent tout utilisateur de drones pour des fins professionnelles (Section I) ; les journalistes ou les personnes utilisant les drones à des fins artistiques ou littéraires (Section II) ; les autorités de l'Etat qui remplissent une mission d'intérêt public (Section III) ; et finalement les particuliers (Section IV).

Section I. Les opérateurs commerciaux

Les opérateurs commerciaux qui traitent des données, doivent respecter la *loi du 8 décembre 1992* relative à la vie privée et le traitement des données. Ils sont soumis aux droits et obligations qui se trouvent dans cette loi. Cependant cette loi présente des carences.

La principale carence de la loi du 8 décembre 1992, est de ne pas répondre adéquatement aux problèmes de sécurité des données posés par les fonctions atypiques des drones. Les drones peuvent : (i) recueillir des données personnelles de

manière accidentelles ; (ii) être facilement ‘hackés’ pas un autre drone ; et (iii) recueillir de vastes données de différents types en un seul vol. En effet, lors de l’utilisation de drones par les opérateurs commerciaux, des d’individus, des plaques d’immatriculation, des champs, des maisons, ou encore des visages de travailleurs peuvent se retrouver sur les images détenues par l’entreprise qui a réalisé les prises ou par l’entreprise qui les a commandé.¹⁹⁶ Ces problèmes sont accentués par le fait que les personnes au sol, repris sur les images, ne sont d’habitude pas avertis de l’utilisation de drones, ou du moins des objectifs poursuivis par l’intervention des drones.¹⁹⁷ Le problème du hacking est propre aux opérateurs commerciaux actifs dans le domaine des télécommunications. La personne malveillante ou l’institution derrière ce piratage informatique pourrait avoir accès à toutes les informations propres aux utilisateurs des services de télécommunications.¹⁹⁸

La législation actuelle, ne contient pas de précision sur le type de mesure de sécurité, organisationnelle ou technique qui doit être prise par les responsables des traitements de données. Cette carence existe tant au niveau de la directive 95/46 qu’au niveau de la loi belge qui en est la transposition. Il n’y a donc pas suffisamment de mesures préventives et de garanties curatives pour prévenir les risques de sécurité inhérents à la technologie des drones pouvant recueillir des données personnels.¹⁹⁹

Outre la loi du 8 décembre 1992, les opérateurs commerciaux doivent aussi respecter l’article 8 de la Convention européenne des droits l’homme, les articles 15, 22, 29, de la Constitution, ainsi que le droit à l’image. Les opérateurs actifs dans les télécommunications doivent également se plier aux prescrits de la loi du 13 juin 2005 sur les communications électroniques.

Section II. Les journalistes ou l’utilisation de drones à des fins artistiques

Le grand danger pour cette seconde utilisation des drones est un usage abusif et intrusif du droit à l’information.

¹⁹⁶ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, p. 175.

¹⁹⁷ *Ibid.*, p. 177.

¹⁹⁸ *Ibid.*, p. 189.

¹⁹⁹ *Ibid.*, pp. 317 et 318.

Comme nous l'avons vu pour ces utilisateurs, la loi du 8 décembre 1992 prévoit des exceptions aux obligations qui s'imposent aux responsables des traitements mais ils doivent toutefois respecter les articles 4 et 5 de la loi. Malheureusement ces exceptions sont trop larges. Il faudrait rappeler qu'une balance est nécessaire entre le droit à la vie privée et les intérêts liés à la liberté d'expression et d'information²⁰⁰. Plutôt que d'accorder des exceptions automatiques, il faudrait définir des critères appropriés à remplir pour bénéficier des exceptions. En outre, la loi de 1992 ne donne aucune interprétation de la notion de « journalisme ». Avec la révolution des médias par l'internet, ce terme soulève des doutes : inclut-il vraiment les « Youtubers », les bloggeurs, ou d'autres internautes qui font passer des informations via internet.²⁰¹

Les journalistes et les artistes sont également tenus de respecter le droit à l'image tel que développé par la jurisprudence, et les articles 15, 22 et 29 de la Constitution.

Section III. Les autorités de l'Etat

Les drones utilisés par les forces de l'ordre peuvent être équipés : (i) de caméras de jours ; (ii) de caméras nocturnes ; (iii) de caméras infrarouge qui détecte les sources de chaleurs ; (iv) de veille infrarouge qui peut détecter et tracer un objet. S'ajoute à cela la possibilité de munir un drone de technologie de reconnaissance faciale. Toutes ces installations sont de nature à interférer avec la vie privée et le traitement de données.²⁰²

Ces autorités assurent l'application de la loi et remplissent des missions de surveillance. Les autorités de l'Etat utilisent majoritairement les drones pour rechercher, traquer et poursuivre des personnes ou des objets, pour recueillir des données personnelles d'une personne dans le cadre de mission de surveillance, et pour surveiller des événements publics.

La loi de 1992 prévoit aussi un régime d'exceptions pour les autorités de l'Etat. Mais comme les journalistes, ils sont soumis aux articles 4 et 5 de la loi. Ils doivent en outre respecter le droit à l'image, l'article 8 de la Convention européenne

²⁰⁰ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, p. 328.

²⁰¹ *Ibid.*, p. 319.

²⁰² *Ibid.*, p. 183.

des droits de l'homme ainsi que certaines facettes de la vie privée, tel que le domicile ou l'intimité de l'individu. Ces prérogatives ont été expressément prévues pour limiter les ingérences excessives dans la vie privée des individus. L'article 148 du Code pénal, peut-être utile si un fonctionnaire s'introduit dans le domicile de l'habitant sans son consentement et hors du prescrit de la loi.

Un déficit dans la législation est l'absence de mise à jour du régime qui s'applique à la surveillance. Celle-ci ne relève pas les défis que posent les nouvelles technologies utilisées par les autorités telles que les drones. La loi prend en compte les captures d'images mais rien n'est dit de la géolocalisation, des données biométriques, de la détection de comportements. Ce manque de provisions expresses pour ces technologies ne permet pas de la légitimer et d'en définir les contours. Cette absence dans la loi signifie aussi que l'impact de ces technologies sur les personnes n'est pas prévisible.

La législation belge prévoit toutefois que pour l'installation de caméras, en plus de l'autorisation de la police et du bourgmestre, il faut prévenir la commission de la vie privée. Celle-ci vérifiera que les données sont traitées dans le respect des droits de la personne concernée. Cependant la Commission ne rend que des avis et des recommandations. Bien que la Belgique soit un des seuls pays européens qui fait référence dans sa législation aux caméras mobiles, la mesure dans laquelle cette législation s'applique aux drones équipés de caméras n'est pas claire. Notre loi n'autorise ces caméras mobiles que dans le cadre de grands rassemblements et dans des lieux ouverts ou fermés mais accessibles au public. Elle ne prend donc pas en compte les lieux fermés non accessibles au public et ne prévoit malheureusement pas l'utilisation des caméras mobiles à d'autres fins que la surveillance de rassemblements. L'utilisation de drones dans des lieux publics à des fins autres que la surveillance d'un grand rassemblement est donc, a priori, interdite en Belgique.²⁰³

Malheureusement le législateur n'a pas précisé dans les travaux préparatoires, ce que la loi vise par les notions de « systèmes d'observation fixes ou mobiles ».²⁰⁴ L'adjectif « mobile » devrait qualifier des caméras qui ne sont pas fixées à un endroit au cours de la surveillance et que l'on déplace durant cette surveillance, par opposition aux caméras « fixes » qui restent au même endroit au cours toute la

²⁰³ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, pp. 320 et 321.

²⁰⁴ C. ATAS et M. DEGROOVER, *op. cit.*, p. 73.

surveillance. La loi pourrait donc à notre avis être complétée de manière plus adaptées aux caméras mobiles et aux nouvelles technologies.²⁰⁵

Section IV. Les particuliers

L'utilisation privée de drones peut facilement se transformer en voyeurisme. Aux vues de la multitude d'informations accessibles sur internet, par l'intermédiaire de forums par exemple, la création ou l'achat de drones est facile et son utilisation est presque accessible à tout un chacun. Cependant, puisque les particuliers sont exemptés des législations, ils constituent sans doute les utilisateurs les plus risqués par rapport aux respect de la vie privée et le traitement des données.²⁰⁶

Les particuliers sont exemptés de l'application de la loi du 8 décembre 1992 quand ils utilisent des drones pour recueillir des données dans l'exercice (i) d'activités exclusivement domestiques, (ii) d'activités ludiques, ou (iii) d'activités personnelles.

Cependant rappelons que l'exemption pour les activités domestiques et personnelles est d'interprétation stricte et que tout dépassement obligera les particuliers à respecter la loi du 8 décembre 1992. Les particuliers doivent également respecter les prescrits de l'article 8 de la Convention européenne des droits de l'homme, ainsi que les articles 15, 22 et 29 de la Constitution. Les particuliers devront aussi respecter le droit à l'image tel que développé par la jurisprudence.

Sous l'angle du droit pénal, aucun article du Code pénal en Belgique ne punit le voyeurisme, comme s'en est ému le collège des procureurs-généraux dans l'affaire de voyeurisme d'un entraîneur de basket²⁰⁷. Le seul article qui pourrait servir de fondement pour le non respect du domicile d'une personne est l'article 439 du Code pénal. Cette disposition prévoit les sanctions lorsqu'un particulier s'introduit dans le domicile d'autrui sans son autorisation, sans ordre de l'autorité, et hors des cas où la loi le permet.

²⁰⁵ C. ATAS et M. DEGROOVER, *op. cit.*, p. 75.

²⁰⁶ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, p. 189.

²⁰⁷ J.C. MATGEN, *Le voyeurisme est-il condamnable en tant que tel?*, 7 mai 2015, <http://www.lalibre.be/actu/belgique/le-voyeurisme-est-il-condamnable-en-tant-que-tel-554b6b3235704bb01c2d9a53>.

CHAPITRE II : PROPOSITION DE REGLEMENT

Nous constatons qu'actuellement les législations présentes sont plutôt curatives que préventives. Il faudrait améliorer l'aspect préventif.

Il existe au niveau européen une proposition de règlement. Nous pensons que l'adoption de ce règlement permettra de diminuer les risques que peuvent soulever l'utilisation de drones par des opérateurs commerciaux. Cette proposition envisage notamment l'introduction : (i) du principe de responsabilité, (ii) des principes de *Privacy by Design et Privacy by Default*, (iii) de l'analyse d'impacts, (iv) d'éclaircissements concernant le principe de minimisation des données²⁰⁸ et (v) d'une obligation de communiquer, à la personne concernée, l'hypothétique violation de ses droits par un opérateur²⁰⁹.

Dans une première section nous analyserons le principe de responsabilité (Section I). Nous examinerons ensuite les principes de protection des données dès la conception et le principe de protection par défaut, ainsi que les analyses d'impacts et des audits (Section II).²¹⁰ Finalement, nous aborderons le droit à l'oubli (Section III).

Section I. L'introduction du principe de responsabilité.

Nous avons vu que les règles qui protègent la vie privée ne sont pas facilement mises en œuvre pour les drones. Le Groupe de travail « article 29 », souligne la nécessité d'avoir des règles mieux adaptées aux technologies, mais surtout, l'introduction d'un principe de responsabilité, afin d'encourager respect de celles-ci²¹¹. Comme l'explique Alain Bensoussan, lorsqu'il s'agit de vie privée, le

²⁰⁸ Art. 5 de la Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données).

²⁰⁹ Art. 32 de la Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données).

²¹⁰ Art. 32 et 33 de la Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données).

²¹¹ Groupe de travail « Article 29 », Opinion 3/2010 on the principle of accountability, Bruxelles, 13 juillet 2010.

principe de responsabilité prend la forme de l'obligation de rapporter et d'expliquer la mise en œuvre des règles, qui répond dès lors aux principes de transparence et de traçabilité.²¹² Ce principe de responsabilité se retrouve à l'article 22 de la proposition de règlement. Le principe tel qu'il est formulé dans la proposition de règlement va permettre d'inverser la charge de la preuve. Le responsable du drone devra être en mesure de prouver à tout moment auprès des personnes concernées par ces traitements, ainsi qu'auprès du public et de l'autorité de étatique constitué à cet effet, son respect des dispositions relatives aux traitements des données. On peut penser que ce principe sera efficace puisque les entreprises qui utilisent des drones seront responsables de prévenir les individus que leurs données ont été traitées. De plus, ce principe de responsabilité aura aussi un impact plus général puisqu'indirectement les entreprises devront aussi continuellement prouver qu'ils respectent tous les prescrits de la loi sur le traitement des données.²¹³

Section II. Les trois améliorations découlant du *soft law*

C'est probablement au niveau du *soft law* que nous trouverons le plus de solutions concernant l'utilisation raisonnable des drones. L'avantage de ce droit est qu'il est flexible, plus pratique, qu'il s'adapte au domaine pour lequel il est adopté et est spécifique à une technologie. Etant neutre technologiquement, les législations sur la vie privée et le traitement des données peuvent être vagues, trop générales, difficiles à comprendre et à mettre en œuvre pour les différentes technologies. C'est pourquoi le *soft law* peut être une solution à notre problème. Nous verrons que des résultats suffisants peuvent découler du principe de protection des données dès la conception, ou du principe d'analyse d'impacts.

²¹² A. BENSOUSSAN, « Accountability and Protection of Personal Data », <http://www.globalprivacybook.com/blog-european-union/306-accountability-and-protection-of-personal-data>

²¹³ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, pp. 324 et 325.

A. Le principe de protection des données dès la conception (Privacy by Design) et par défaut (Privacy by Default)

A.1 Privacy by Design

Ce principe consiste à protéger la vie privée en incorporant cette protection dans les spécifications de conception, dans les pratiques du business, et dans les infrastructures du réseau. Ce principe n'est pas prévu dans la directive actuelle 95/34/CE mais l'est dans la proposition de règlement. Ce principe permettra d'impliquer les designers, les développeurs, et les constructeurs de drones. Le but est donc de transférer une partie des responsabilités qui repose aujourd'hui entièrement sur les épaules du responsable du traitement des données à ceux qui développent les spécifications techniques et ceux qui construisent le drone ou le software qui le contrôle.²¹⁴ Cela permet aussi d'éviter que ceux-ci ne soient uniquement motivés par le profit.

Dans le *Privacy by Design*, le responsable du traitement devra, tant lors de la définitions des moyens qui seront mis en œuvre que lors du traitement proprement dit, appliquer des techniques appropriées pour que les traitements soient conformes aux principes du règlement et respectent les droits de la personne concernée par le traitement²¹⁵.

Le Groupe de travail « Article 29 », soutient dans un avis que l'application du principe *Privacy by Design* peut aider à mieux respecter de la vie privée et les règles en matière traitement des données à caractère personnel²¹⁶. Le Groupe de travail a répondu à des questions sur les drones en identifiant des mesures qui peuvent être utilisées dans le cas des drones pour respecter ce principe de *Privacy by Design* et donc la vie privée. En cas d'usage de drones avec des caméras, des techniques d'anonymisation pourraient être mis en œuvre par les utilisateurs de drones pour rendre les images flous ou d'autre effets graphiques afin de prévenir que des images de personnes soient récoltées alors que ce n'est pas indispensable. Suivant le but de

²¹⁴ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, pp. 329 et 330.

²¹⁵ Art. 23 de la Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), 25 janvier 2012.

²¹⁶ R. Wong, « The Future of privacy », *Computer Law and Security Review*, 2010, p.3, trouvé sur http://works.bepress.com/rebecca_wong/12/.

l'utilisation du drone, les images pourraient être cachées lors qu'elles sont collectées, décodées uniquement lorsque c'est nécessaire, et mises à la dispositions que des personnes autorisées.²¹⁷

Le principe *Privacy by Design* a l'avantage d'être préventif, ce qui est essentiel dans le contexte des drones. On sait que les drones s'accordent difficilement avec le principe de minimisation et de transparence. Pour adopter des technologies qui respectent ces principes, on pourrait, par exemple, concevoir une caméra qui permet de flouter les visages. Ceci permet aux exploitants de drones d'éviter les risques de non-respect dès le départ, et réduire la charge financière et administrative d'informer, par après, les individus à propos de la collecte de leurs données personnelles.²¹⁸

La Commission vie privée précise que le concept de *Privacy by Design* est adapté à la technologie des drones. Les constructeurs intègrent des modalités techniques propres à l'usage particulier du drone. Ces modalités interdisent l'opérateur d'utiliser le drone pour un autre usage que celui prévu initialement.²¹⁹ La Commission cite, à titre d'exemple, plusieurs applications concrètes de ce principe : (i) équiper uniquement le drone par exemple d'une caméra longue portée est disproportionné pour un usage strictement domestique ; (ii) adapter la technologie embarquée, en mettant en place des techniques de floutage automatique des visages par exemple ; (iii) mettre en place un système de sécurisation des données pour éviter tout accès non autorisé à celles-ci ; (iv) prévoir de l'information générale par le biais de manuels, sites internet, formations.²²⁰

Un autre exemple de l'application du Privacy by Design est la « Smart surveillance ». Comme nous l'avons vu la « Smart surveillance » récemment développée, permet de limiter le nombre de données collectées, notamment en

²¹⁷ Groupe de travail « Article 29 », Remotely Piloted Aircraft Systems (RPAS) – Response to the Questionnaire, European Commission, Bruxelles, Décembre 2013, p. 3 trouvé sur http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20131216_reply_to_rpas_questionnaire.pdf.

²¹⁸ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, pp. 331 et 332.

²¹⁹ Commission de la protection de la vie privée, « Questions les plus fréquemment posées – Drones », FAQ 2014, <http://www.privacycommission.be/fr/faq-page/7346#t7346n16588>.

²²⁰ Commission de la protection de la vie privée, « Questions les plus fréquemment posées – Drones », FAQ 2014, <http://www.privacycommission.be/fr/faq-page/7346#t7346n16588>.

utilisant des gâchettes et des filtres qui bloquent des centaines données ou transmettent des images limitées.²²¹

A2. Privacy by Default.

Dans la proposition de règlement on retrouve aussi le principe de *Privacy by Default*. Au travers de ce mécanisme, sont incorporés les principes de proportionnalité et de minimisation.²²² Comme nous le savons, le principe de proportionnalité exige que le traitement des données soit proportionnel à la portée et aux objectifs poursuivis et le principe de minimisation impose aux opérateurs d'utiliser la technique la moins invasive se limiter à la collection du minimum d'information nécessaire pour le but poursuivi²²³.

B. L'analyse d'impacts relatifs à la vie privée

L'analyse d'impacts est un processus d'évaluation des effets potentiels d'une mesure, d'un projet ou d'une législation sur la vie privée et les libertés des personnes du fait de leur nature, de leur portée ou de leur finalités.²²⁴ Dans le contexte des drones, ce concept obligerait le responsable du traitement ou le sous-traitant agissant pour son compte de procéder à une analyse des impacts des traitements envisagés sur la vie privée, la sécurité, les risques de cette technologie.²²⁵

Nous pensons que c'est un outil préventif essentiel pour l'industrie du drones, qui permettra d'augmenter la transparence, la confiance des individus et la protection de leur droit. Ces analyses peuvent aussi contribuer à la gestion des risques de la transgression de droits.²²⁶

Imposer ces analyses à différents niveaux, que ce soit au stade de la conception des drones ou des technologies ou lors du traitement des données par le

²²¹ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, p. 183.

²²² *Ibid.*, p.76.

²²³ *Ibid.*, p.71.

²²⁴ PIAF Project, *A Privacy Impact Assessment Framework*, 2012, <http://www.piafproject.eu>.

²²⁵ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, p. 334.

²²⁶ D. WRIGHT, M. FRIEDEWALD, S. GUTWIRTH, M. LANGHEINRICH, E. MORDINI, R. BELLANOVA, P. DE HERT, K. WHADWA et D. BIGO, *Op. cit.*, p. 16, trouvé sur http://works.bepress.com/serge_gutwirth/69/.

responsable, serait une bonne chose. Mais ce serait encore mieux de couler cette obligation d'analyse d'impacts dans une loi. La vérification de ces analyses devrait être soumise aux autorités de la vie privée, c'est à dire en Belgique la Commission de la vie privée.²²⁷

La proposition de règlement oblige de procéder à ces analyses lorsque des traitements sont susceptibles d'impliquer des risques pour la vie privée. Il faut se demander si une telle analyse ne devrait pas être imposée chaque fois qu'une nouvelle technologie intrusive (par exemple un nouveau drone) voit le jour.

Dans un avis sur les technologies biométriques de 2012, le Groupe de travail « Article 29 » recommande que celui qui définit la destination et les moyens de l'appareil, qu'il soit fabricant, assembleur ou utilisateur final, analyse l'impact de cet appareil sur la vie privée. Le Groupe recommande encore de prendre en compte pour les analyses : (i) la nature des données collectées ; (ii) le but en vue duquel ces données sont collectées ; (iii) la précision de la technologie ; (iv) la base légale, et le respect de celle-ci, un éventuel consentement s'il est nécessaire ; (v) les personnes ayant accès au système qui récolte les informations et aux informations elles-mêmes, et si des mesures sont prises pour protéger l'accès aux informations ; (vi) l'existence de moyens moins intrusifs pouvant être utilisés ; (vii) la durée pendant laquelle les données sont gardées et quand elles sont supprimées ; (viii) le droit des sujets du traitement.²²⁸ Nous estimons toutefois que ces différents points à prendre en compte pour les données biométriques peuvent tout autant s'appliquer à d'autres technologies dont les drones peuvent être équipés. Il serait utile de compléter ces points en prenant aussi en compte la capacité du drone et le type de données spécifiques qui sont traitées.

On peut conclure que les analyses d'impacts augmentent la confiance des individus, puisque ces analyses augmentent la transparence. En effet, tout individu saura quels sont les risques des différentes technologies, à quelle fin leurs informations sont traitées et aura ainsi une meilleure visibilité sur le processus de ce traitement.

²²⁷ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, p. 337.

²²⁸ Groupe de travail « Article 29 », Opinion 3/2012 on developments in biometric technologies, 00720/12/EN WP193, 27 avril 2012, p. 29 et 30.

C. L'audit privé

« L'audit en matière de vie privée a pour objectif de guider les entreprises et les administrations dans leur travail de mise en conformité à la législation relative à la vie privée et à la protection des données personnelles. Il consiste à décrire avec précision les traitements de données qui sont réalisés dans le cadre de leur activité quotidienne et à les analyser en toute objectivité et indépendance au regard des règles applicables, afin d'identifier les mesures correctives qui doivent être prises »²²⁹.

L'analyse d'impacts et l'audit ont le même objectif qui est d'identifier et de contrôler les risques pour prévenir la violation des lois sur la vie privée.²³⁰

Les Audites privées sont reprises à l'article 22 paragraphe 3 de la proposition de règlement. On pourrait donc prévoir que minimum une fois par an des audits soient prévues pour les entreprises impliquées dans le domaine des drones pour évaluer et renforcer leur système de protection des données personnelles.²³¹

Section III. Reconnaissance d'un droit à l'oubli

La proposition de règlement renforce les droits individuels de la personne dont les données sont traitées en prévoyant à l'article 17 un droit à l'oubli numérique et un droit à l'effacement. Ces droits sont nés de l'interprétation de la Cour de justice des articles 12 et 14 de la directive 95/46/CE. Dans cet arrêt²³², la Cour a conclu que Google, au même titre que tout autre moteur de recherche, exploite des données personnelles au sens du droit européen. Ainsi, les obligations liées à ce droit en

²²⁹ C. GOBLET, « Audit en matière de vie privée & de données à caractère personnel », 2015, http://www.lexconsult.pro/avocat_services/audit-de-conformite-legislation-vie-privee-et-donnees-a-caractere-personnel.php.

²³⁰ R. CLARKE, « Privacy impact Assessments », 2015, <http://www.rogerclarke.com/DV/PIA.html>.

²³¹ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, p. 342.

²³² C.J.C.E., 13 mai 2014 (Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González), C-131/12, <http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=fr&mode=lst&dir=&occ=first&part=1&cid=287400>.

matière de gestion et de suppression leur sont applicables. La reconnaissance par la Cour, au nom de la vie privée, qu'une personne puisse demander la suppression de données liées à leur nom dans une liste de résultats affichée à la suite d'une recherche effectuée à partir du nom de cette personne, au motif que ces informations sont susceptibles de lui porter préjudice ou qu'elle désire que celles-ci soient «oubliées» après un certain temps, consacre un droit à l'oubli ou à l'effacement numérique.²³³

CHAPITRE III : DROIT COMPARE

Dans ce chapitre, nous analyserons le système juridique de la France puisque ce pays est déjà doté d'une législation spécifique aux drones (Section I) et également les Etats-Unis en tant que première nation utilisatrice et constructrice de drones²³⁴ (Section II).

Section I. La législation française.

A. Cadre juridique

La France depuis quelques années s'est équipée de deux arrêtés du 11 avril 2012²³⁵ :

- (i) l'un relatif à la conception des drones civils, aux conditions d'utilisation, et les capacités requises pour les personnes qui les utilisent ;
- (ii) l'autre arrêté est relatif à l'utilisation de l'espace aérien par les drones.

En outre la législation française contient (i) l'article L6113-2 du Code des transports qui prévoit la responsabilité du pilote en cas de dommages causés par son drone ou par les objets qui s'en détachent ; (ii) l'article L6232-4 du même code portant sur les dispositions pénales liées à l'utilisation du drone en violation des règles de

²³³ C.J.C.E., 13 mai 2014 (Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González), C-131/12, <http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=fr&mode=lst&dir=&occ=first&part=1&cid=287400>.

²³⁴ S. ROGERS, *Drones by country : who has all the UAVs ?*, 3 août 2012, <http://www.theguardian.com/news/datablog/2012/aug/03/drone-stocks-by-country>.

²³⁵ Arrêté du 11 avril 2012 relatif à la conception des aéronefs civils qui circulent sans aucune personne à bord, aux conditions de leur emploi et sur les capacités requises des personnes qui les utilisent ; Arrêté du 11 avril 2012 relatif à l'utilisation de l'espace aérien par les aéronefs qui circulent sans personne à bord.

sécurité ; (iii) l'article D133-10 du Code de l'aviation traitant spécifiquement des prises de vues aériennes ; (iv) finalement il existe aussi un article du Code pénal qui prévoit la sanction du non respect de la vie privée.²³⁶ Cependant, la majorité de ces réglementations concerne essentiellement la sécurité en ne traite pas de la protection de la vie privée, à l'exception de l'article du Code pénal.

B. Protection de la vie privée

Se pose alors la question de l'existence en droit français de règles spécifiques à la protection de la vie privée lors de l'utilisation de drones.

B.1 Dispositions générales

Tout d'abord on retrouve le droit à la vie privée dans l'article 2 de la Déclaration des Droits de l'Homme et du Citoyen de 1789 et à l'article 9 du Code civil.²³⁷

B.2 Dispositions propres aux types d'utilisations

La loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés règle le traitement de données à caractère personnel. Elle s'applique aussi bien aux données traitées par le secteur public que le privé.²³⁸ L'article 2 exempte les traitements de données réalisés à des fins personnelles ou domestiques²³⁹. A l'inverse de la loi belge du 8 décembre 1992, la loi ne prévoit pas d'exception pour les traitements à des fins journalistiques et artistiques ou par les autorités de l'Etat²⁴⁰.

L'utilisation de drones à des fins de communication doit respecter l'ordonnance du 24 août 2011 relative aux communications électroniques²⁴¹. L'ordonnance requiert du fournisseur du réseau qu'il assure la confidentialité des

²³⁶ D. SANZ, Drones: *que dit la loi?*, 24 février 2015, le figaro, <http://www.lefigaro.fr/actualite-france/2015/02/24/01016-20150224ARTFIG00147-drones-que-dit-la-loi.php>.

²³⁷ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, p. 93.

²³⁸ *Ibid.*, p. 94

²³⁹ Art. 2 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624&dateTexte=vig-%3Ehttp://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624&dateTexte=vi>

²⁴⁰ Art. 26, 41 et 67 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624&dateTexte=vig-%3Ehttp://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624&dateTexte=vi>

²⁴¹ Ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques

communications et qu'il supprime ou anonymise les données de trafic relatives aux communications. Les données de localisation relatives aux communications ne peuvent pas être traitées ou enregistrées sans le consentement de la personne concernée par le traitement.²⁴²

Il y a plusieurs lois qui sont applicables aux drones civils utilisés à des fins de surveillance. Pour la vidéosurveillance l'installation de caméras dans des lieux publics est une prérogative des autorités publiques, qui seules sont compétentes²⁴³. Les autorités devront respecter (i) les articles L223-1 et L251-1 du Code de la sécurité intérieure ; (ii) la loi du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure²⁴⁴ et plus spécifiquement l'article 18 qui prévoit les situations dans lesquels la surveillance est permise; (iii) la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ; (iv) l'article 226-1 du Code pénal.²⁴⁵ Malheureusement ces législations ne contiennent aucune précision sur les caméras mobiles. Ensuite, pour la surveillance réalisée par les forces de l'ordre, on peut imaginer que ces autorités utilisent des drones civils pour accéder aux contenus des téléphones mobiles, des ordinateurs, et ensuite intercepter les communications. Dans ces circonstances, ils devront respecter la loi du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure²⁴⁶. Finalement, la surveillance par drones de la police est aussi soumise à la loi sur la géolocalisation²⁴⁷ ainsi que la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés²⁴⁸, si le drone est équipé d'un système permettant de collecter les données de localisation de quelqu'un ou suivre une cible.²⁴⁹

²⁴² R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, p. 95.

²⁴³ *Ibid.*, p. 96.

²⁴⁴ Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure
<http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023707312&categorieLien=id>

²⁴⁵ Commission nationale de l'information et des libertés,
http://www.cnil.fr/fileadmin/documents/approfondir/dossier/Videosurveillance/CNIL_Video_voie_publique.pdf.

²⁴⁶ Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure
<http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023707312&categorieLien=id>

²⁴⁷ Loi n° 2014-372 du 28 mars 2014 relative à la géolocalisation

²⁴⁸ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

²⁴⁹ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, p. 98.

Enfin, l'article L226-1 du Code pénal détermine les peines en cas d'atteinte à l'intimité de la vie privée d'autrui, en révélant des paroles prononcées à titre privé ou l'enregistrement ou la transmission de l'image d'une personne sans son consentement.

En conclusion par rapport à la Belgique, la France s'est déjà munie d'une législation relative aux drones et punit pénalement la violation du droit à l'image. Par contre, la France, à l'inverse de la Belgique, dans sa législation relative à la vidéosurveillance, ne traite pas des caméras mobiles.

Section II. La législation américaine

Tout comme l'Union européenne, l'Etats-Unis ont adopté une *Roadmap* et ont annoncé l'arrivée de 30.000 drones civils dans l'espace aérien national dans moins de vingt ans²⁵⁰.

Pour l'instant la *Federal Aviation Administration* (FAA) a autorisé des entités publiques telles que des agences fédérales, des universités et des polices locales, d'utiliser des drones au cas par cas. Les utilisateurs commerciaux ont tenté d'obtenir des autorisations mais ils n'ont obtenu des autorisations que pour des tests. Le gouvernement est actuellement entrain d'examiner comment renforcer sa législation en matière de vie privée. Au niveau fédéral, de nombreux projets de lois à ce sujet ont été déposés au cours des 112^e et 113^e Congres²⁵¹.

La vie privée et la protection du traitement de données se sont développées à partir de la jurisprudence et aussi du quatrième amendement de la Constitution des Etats-Unis. Ce quatrième amendement garantit aux citoyens un degré de vie privée contre les intrusions du gouvernement. La législation sur la vie privée applicable aux drones dépend de leur utilisation par le gouvernement ou par des entités privés.²⁵²

²⁵⁰ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, p. 131.

²⁵¹ J. VILLASENOR, « Observations from above: Unmanned Aircraft Systems and Privacy », *Harvard Journal of Law & Public Policy*, Vol. 36 N° 2, 2012, p. 509, http://www.harvard-jlpp.com/wp-content/uploads/2013/04/36_2_457_Villasenor.pdf.

²⁵² R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, p. 132.

A. Pour les drones commerciaux ou privés

Le premier moyen d'action qui peut être introduit devant les cours et tribunaux repose sur la notion de l'intrusion. L'intrusion est reliée à la protection de la vie privée et permet à son titulaire de restreindre l'introduction illégale et non autorisée sur sa propriété. Ceci pourrait être utile pour éviter que les drones ne volent au dessus de la propriété de quelqu'un.²⁵³

En plus de l'intrusion, le droit moderne de la responsabilité civile américaine comprend quatre catégories d'ingérence dans la vie privée : (i) l'intrusion dans la solitude, qui comprend tout intrusion physique ou électronique dans la sphère privée d'une personne; (ii) la divulgation publique de faits privés ; (iii) la fausse représentation de la personne; et (iv) l'appropriation. De plus, la protection de la vie privée peut également s'opérer sur base de plaintes pour harcèlement.²⁵⁴

B. Les drones gouvernementaux

Le sacro-saint quatrième amendement de la Constitution des Etats-Unis et sa jurisprudence peuvent constituer une limite à l'utilisation de drones gouvernementaux dans des activités de surveillances, surtout lors de perquisitions. Cet amendement confère un droit aux citoyens de ne pas être perturbé dans leur vie privée par les perquisitions du gouvernement. La question qui nous intéresse est de savoir si la surveillance par drone par le gouvernement constitue une perquisition, une recherche intrusive nécessitant un mandat et le respect des protections conférées par les garanties du *4th Amendment*. Malgré que la Cour Suprême des Etats-Unis n'ait, à ce jour, pas encore été confrontée à des questions sur les drones, on peut relever quelques exemples de jurisprudences qui pourraient nous éclairer sur la nécessité d'un mandat ou non pour certaines activités de surveillance.²⁵⁵

²⁵³ J. VILLASENOR, *op. cit.*, p. 499.

²⁵⁴ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, p. 132.

²⁵⁵ R. M. THOMPSON II, *Drones in Domestic Surveillance Operations: Fourth Amendment Implication and Legislative Response*, Congressional Research Service, Report for Congress, 2013, p. 4, <https://www.fas.org/sgp/crs/natsec/R42701.pdf>.

Dans les arrêts, *California v. Ciraolo*²⁵⁶, *Florida v. Riley*²⁵⁷ et *Dowe Chemical v. United States*²⁵⁸, la Cour a décidé que de la surveillance comprenant la photographie de zones visibles ouvertes, prise d'un avion avec un pilote muni d'un appareil conventionnel, ne constitue pas une perquisition sous le quatrième amendement et ne requiert donc pas un mandat, puisque ces zones sont ouvertes au regard du public.²⁵⁹ Dans l'arrêt *Kyllo v. United States*²⁶⁰, la Cour conclut que l'utilisation de technologies telle que des caméras thermiques, pour recueillir des informations relatives à l'intérieure d'une maison constitue une intrusion dans la vie privée, et ainsi constitue une perquisition sous le quatrième amendement qui nécessite un mandat. Le fait de surveiller la localisation et les mouvements d'une personne par un GPS accroché à une voiture requiert également un mandat.²⁶¹

Il ne semble donc pas claire quand une surveillance par drone, constituera une perquisition au sens du quatrième amendement et nécessitera un mandat. Toutefois on peut remarquer que cela dépendra de: (i) les attentes de la société en matière de vie privée par rapport à l'endroit perquisitionné ; (ii) l'endroit surveillé ; (iii) la technologie utilisée ; (iv) la durée de la surveillance.²⁶²

La *Unwarranted Surveillance Act*²⁶³ de 2013 stipule que les autorités de l'Etat doivent avoir un mandat pour les activités de surveillances par drones, mais cette loi n'a pas encore été adoptée²⁶⁴.

Paradoxalement on remarque que les Etats-Unis, bien qu'étant le premier pays en nombre de drones, ne comprend à l'heure actuelle aucune législation spécifique qui protège la vie privée des citoyens contre les drones. Seule la responsabilité civile ou la

²⁵⁶ US Supreme Court, *California v. Ciraolo*, 476 U.S. 207 (1986), <https://supreme.justia.com/cases/federal/us/476/207/>.

²⁵⁷ US Supreme Court, *Florida v. Riley*, 488 U.S. 445 (1989), <https://supreme.justia.com/cases/federal/us/488/445/case.html>.

²⁵⁸ US Supreme Court, *Dow Chemical Co. v. United States*, 476 U.S. 227 (1986), <https://supreme.justia.com/cases/federal/us/476/227/case.html>.

²⁵⁹ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, p. 133.

²⁶⁰ US Supreme Court, *Kyllo v. United States*, 533 U.S. 27 (2001), <https://supreme.justia.com/cases/federal/us/533/27/case.html>.

²⁶¹ US Supreme Court, *United States v. Jones*, 565 U.S. (2012), <https://supreme.justia.com/cases/federal/us/565/10-1259/>.

²⁶² R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, p. 134.

²⁶³ Unwarranted Surveillance Act of 2013, S.1016 — 113th Congress (2013-2014).

²⁶⁴ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, p. 134.

jurisprudence du quatrième amendement permettent de recevoir des demandes basées sur le non respect de la vie privée.

CHAPITRE IV : AMELIORATIONS POSSIBLES DU CADRE JURIDIQUE DES DRONES

Dans ce chapitre nous verrons les différentes mesures qui peuvent être mises en œuvre pour s’assurer que la Belgique se dote d’un cadre juridique qui préserve la sécurité de ses citoyens et sauvegarde leurs droits et libertés fondamentales. De la sorte, les drones seront plus facilement acceptés par l’opinion publique. Nous avons appris qu’un projet d’arrêté royal relatif à l’utilisation de drones est actuellement en phase d’adoption.²⁶⁵ Cet arrêté traite essentiellement de la sécurité et de l’encadrement de l’usage des drones dans l’espace aérien belge. En terme de protection de la vie privée, l’arrêté renvoie aux dispositions légales applicables en matière de vie privée.²⁶⁶

Dans ce chapitre, nous identifierons les améliorations qui pourraient être apportées, notamment par le projet d’arrêté royal, au cadre législatif belge pour les professionnels (Section I), ainsi que pour les particuliers (Section II). Finalement nous verrons des mesures plus générales que le cadre juridique devrait inclure (Section III).

Section I. Les professionnels

A. La licence

Nous avons appris qu’un arrêté royal, actuellement en phase d’adoption, prévoit l’introduction d’une licence de vol pour les drones. Aucun professionnel ne pourra voler avec un drone s’il n’est pas possesseur d’une licence. Cette licence comprendrait un test de connaissance théorique mais également un test d’aptitude pratique. Tout comme le permis de voiture on pourrait prévoir une licence par catégorie adaptée aux différents types de drones²⁶⁷. L’utilisateur de drones aura ainsi

²⁶⁵ Arrêté royal relatif à l’utilisation des aéronefs télé pilotés dans l’espace aérien belge.

²⁶⁶ Voy. Annexe 1, point 9.

²⁶⁷ La licence sera en fonction du type de drone utilisé lors de l’épreuve pratique, Espace Drone, Manuel théorique du pilote de RPAS, 1^{er} édition, Belgique, 2014, p. 15.

une formation complète sur son type de drone et sera apte à évaluer tous les risques que son drone comporte, aussi bien au niveau de la sécurité, qu'au niveau de la protection de la vie privée. Il serait fortement recommandable de donner, lors des formations théoriques, une initiation aux différentes législations concernant la vie privée et le traitement des données. En effet, cela permettrait à chaque licencié de connaître le cadre légal relatif à la vie privée, et de le sensibiliser à d'éventuels contraventions à la vie privée.²⁶⁸ Pour la licence nous pensons, qu'il serait bénéfique, que le professionnel aie des connaissances : (i) météorologiques ; (ii) aérodynamiques ; (iii) des règles aéronautiques ; et (iv) des facteurs humains.²⁶⁹

B. L'assurance

L'arrêté ayant comme préoccupation première la sécurité, il imposera fort probablement que les utilisateurs professionnels soient munis d'une assurance responsabilité civile. Cette assurance couvrirait les dommages corporels et matériels fait à des tiers suite à une chute de drones ou un accident.

C. Manuel d'exploitation et analyse d'impacts

Monsieur Mascart, Vice Président de la *Belgium Unmanned Aircraft System Association* (BeUAS)²⁷⁰ a relevé l'existence en France, comme en Allemagne, du concept d'analyse d'impacts pour les vols à risques. Dans ces pays, les analyses pour les vols à risque permettent d'identifier des scénarios catastrophes en terme de sécurité et d'évaluer les mesures à prendre.²⁷¹ Il serait bénéfique de prévoir en Belgique, pour les vols à risques, des analyses au niveau sécuritaire mais également au niveau la vie privée. Par vol à risque il faut entendre tout vol : (i) qui peut s'avérer risqué du à l'environnement dans lequel il a lieu ; (ii) où la sécurité des tiers au sol est susceptible d'être compromise ; où encore (iii) qui par sa mission peut s'avérer risqué pour les tiers au sol.

Cependant, notons que dans le système belge actuel, Espace Drone, l'école travaillant en connivence avec la Direction Générale de Transport Aérien (DGTA)

²⁶⁸ Voy. Annexe 1, point 5.

²⁶⁹ Voy. Annexe 2, point 8.

²⁷⁰ Cette personne a été interrogé en sa position de Vice Président de BeUAS. Voir la retranscription de l'entrevue en Annexe 1.

²⁷¹ Voy. Annexe 1, point 4.

enseigne, dans son syllabus, que chaque exploitant de drone doit établir un manuel d'exploitation. Ce manuel contient toutes les informations et les instructions relatives à un drone nécessaire pour une utilisation correcte et en toute sécurité. A titre d'exemple, il est requis d'inclure dans ce manuel (i) la procédure de contrôle de l'aéronef en vol, (ii) les procédures de sécurité, (iii) la procédure de notification, d'examen et de suivi d'un accident ou incident, (iv) les procédures relatives aux exécutions spécialisées à haut risque. Ces dernières comprennent une analyse des dangers, une évaluation des risques et une description des mesures de prévention. De la sorte, ces informations contenues dans le manuel d'exploitation se rapprochent du mécanisme d'analyse d'impacts prévu dans la proposition de règlement.²⁷²

D. Mesures de sécurité

L'Arrêté royal, comme l'a souligné Greg Billen, pourrait prévoir plusieurs mesures qui permettraient d'assurer une utilisation sécurisée des drones. Premièrement, il faudrait exiger des professionnels que leurs drones soient contrôlables si un rotor est hors service. Pour les vols à risques cette exigence pourrait être portée à deux rotors. Les professionnels devraient d'ailleurs utiliser des drones avec plus de quatre rotors car les drones à quatre rotors ne sont plus contrôlables si un seul des rotors est hors service. Finalement, cette interdiction des drones à quatre rotors pour les professionnels permettrait aussi d'éviter qu'un particulier utilise son drone à des fins professionnelles et ainsi permet d'éviter le travail non déclaré.²⁷³

Au niveau de l'altitude, l'exigence de 300 pieds pour les professionnels (91 mètres), prévues initialement par l'Arrêté, est trop basse dans la mesure où certains drones, comme le modèle « aile » fréquemment utilisé pour la cartographie, nécessite une altitude égale ou supérieure à 110 mètres pour être efficace. Il faudrait interdire aux hélicoptères de descendre en dessous de 200 mètres et prévoir une altitude maximale pour les drones professionnels de 150 mètres.²⁷⁴

Finalement une mesure efficace pour la sécurité serait d'équiper les drones professionnels de transpondeurs équivalents à ceux utilisés par l'aviation. Ceci

²⁷² Espace Drone, Manuel théorique du pilote de RPAS, 1^{er} édition, Belgique, 2014, p. 7.

²⁷³ Voy. Annexe 2, point 3.

²⁷⁴ Voy. Annexe 2, point 7.

permettrait de localiser chaque drone et d'identifier son pilote. De cette manière, il serait facile de contrôler si le pilote est possesseur d'une licence. Enfin, munir les drones d'un transpondeur permettrait aussi de mettre en place un site détectant les drones présents dans l'espace aérien, tel que le site www.flightradar24.com qui permet de tracer les avions en temps réel. Cette mesure augmenterait la transparence et faciliterait l'approbation dans l'opinion publique de l'usage des drones.²⁷⁵

E. Devoirs et responsabilité de l'exploitant

Le cadre juridique devrait mettre en place un régime spécifique de devoirs et de responsabilité. Ce régime pourrait imposer notamment les obligations : (i) chaque vol doit avoir lieu selon la procédure décrite dans le manuel d'exploitations, (ii) l'exploitant doit garantir la sécurité des opérations entreprises, (iii) l'exploitant doit se munir d'une police d'assurance adéquate couvrant chaque vol, (iv) l'exploitant doit se soumettre à la surveillance de la DGTA et fournir tous les renseignements nécessaires à cette surveillance, et (v) l'exploitant doit veiller à traiter les données à caractère personnel conformément à la réglementation en vigueur.

Section II. Les particuliers

A. Limitations techniques

L'Arrêté royal n'exige pas de licence pour les particuliers mais propose de soumettre les vols à une limite d'altitude. Initialement, l'Arrêté envisageait une altitude maximale. Monsieur Mascart pense que c'est une mauvaise idée car la mise en œuvre semble difficile. Il est d'avis qu'une limitation par le poids ou d'autres données technologiques seraient plus réalistes.²⁷⁶ Pour Monsieur Billen, l'attitude maximale de 100 pieds (30 mètres) pour les particuliers est suffisante. Ce dernier ne rejette pas l'idée d'une limite de poids mais souligne qu'un kilo, comme le prévoit la France par exemple, est vite dépassée.²⁷⁷ L'Arrêté devrait prévoir qu'en cas de dépassement du poids, le pilote doivent être titulaire d'une licence semblable à celle des professionnels.

²⁷⁵ Voy. Annexe 2 point 9.3.

²⁷⁶ Voy. Annexe 1, point 7.

²⁷⁷ Voy. Annexe 2 point 3 ; Art. 4 de l'Arrêté du 11 avril 2012 relatif à la conception des aéronefs civils qui circulent sans aucune personne à bord, aux conditions de leur emploi et sur les capacités requises des personnes qui les utilisent.

Une dernière limite serait de limiter les drones des particuliers à quatre rotors. Cette mesure faciliterait le contrôle de l'utilisation des drones fins professionnels ou particuliers, et accessoirement permettrait d'éviter le travail non déclaré²⁷⁸.

B. Responsabilité

En terme de responsabilité, les victimes de drones peuvent recourir au droit commun de la responsabilité extracontractuelle (l'article 1384, al. 1^{er} – de la responsabilité du fait des choses) pour avoir leurs dommages réparés par le propriétaire ou gardien du drone.

Section III. Mesures générales envisageables pour compléter le cadre juridique régissant les drones

A. Territoire survolable

Une fois l'Arrêté rentré en vigueur, seul un quart ou un cinquième du territoire belge sera survolable sans autorisation pour les professionnels ayant une licence ou les particuliers respectant les limites techniques. Le reste du territoire correspond à des zones d'exclusion : aéroport (zones CRT), ou zones militaires. Ces zones d'exclusions sont interdites aux particuliers et soumises à l'obtention d'une autorisation au cas par cas pour les professionnels. Il est impératif que le législateur établisse une carte claire détaillant les différentes zones. Comme aux Etats-Unis on pourrait brouiller les ondes radios utilisées pour piloter les drones afin d'empêcher le survole de certaines zones à risque, ou non autorisées.

B. Améliorations tirées du droit communautaire

Comme nous l'avons déjà vu, la proposition de règlement comprend plusieurs aspects du *soft law* pertinent pour le cadre législatif belge. Premièrement, le principe de *Privacy by Design* peut être utile pour réglementer de manière préventive les drones et pour limiter l'utilisation de ceux-ci à leur usage initial. Des lignes directrices précisant les éléments essentiels de ce principe faciliteraient sa

²⁷⁸ Voy. Annexe 2, point 3.

compréhension et sa mise en œuvre par les constructeurs, les designers et les utilisateurs.²⁷⁹

Un second aspect intéressant tiré du droit communautaire est l'autorégulation. Elle est définie par la Commission européenne comme la possibilité pour les acteurs économiques, les partenaires sociaux, les organisations non-gouvernementales, ou les associations d'adopter entre eux et pour eux des lignes directrices au niveau européen (spécialement des codes de conduite, ou des accords de secteur). Ces règles sont non liantes et d'interprétation libre. Leur objectif est de promouvoir des comportements en impliquant les parties prenantes et en établissant des règles par la communauté intéressée par leur utilisation (*bottom-up*).²⁸⁰ Elles sont généralement élaborées par les autorités, par les entreprises et par les organisations industrielles. Ainsi, l'autorégulation pourrait s'appliquer à chaque niveau de l'industrie du drone, du constructeur à l'utilisateur. La directive actuelle 95/46/CE encourage d'ailleurs l'adoption de l'autorégulation dans son préambule dans lequel elle stipule que les Etats membres doivent favoriser les milieux professionnels à élaborer des codes de conduite, pour la mise en œuvre de la directive. Développer un code des pratiques permet de (i) avoir des règles sur mesure, spécifiques à une technologie ; (ii) dresser des exemples pratiques ; (iii) rendre les règles de respect de la vie privée et des traitements des données plus accessibles aux producteurs et aux utilisateurs de drones. Par exemple, en adoptant de tels codes, les autorités de la protection de la vie privée donneraient des informations précises aidant les acteurs dans l'industrie des drones à mieux comprendre comment appliquer les lois protégeant la vie privée.²⁸¹

Finalement, en adaptant de telles règles l'industrie du drones envoie un signal au public qu'elle se soumet à ses obligations en matière de vie privée. Ce mécanisme renforce aussi le respect du principe de transparence et indirectement améliore la perception des drones dans l'opinion publique.

On peut aussi penser pour les particuliers que les clubs de modélisme adoptent des codes de conduite dans lesquels ils peuvent promouvoir le respect de la vie privée,

²⁷⁹ R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, p. 333.

²⁸⁰ *Ibid.*, p. 342.

²⁸¹ *Ibid.*, p. 344.

en interdisant à leurs membres, par exemple, de munir leur drones de caméras infrarouge ou tout autre équipement intrusif pouvant poser de graves problèmes de protection des données à caractère personnel.²⁸²

C. Améliorations tirées du droit comparé

Comme nous l'avons vu, la France comme les Etats-Unis ne disposent pas d'une protection plus élevée de la vie privée propre aux drones que la Belgique. Certains éléments des deux arrêtés de droit français portant sur la question de la sécurité liée aux drones pourraient être repris dans notre droit interne. En outre, la construction jurisprudentielle du droit à l'image pourrait être renforcée dans notre système juridique belge en consacrant un article pénal sanctionnant le non respect du droit à l'image, à l'instar du droit français.

D. Autres mesures techniques de prévention

Certaines techniques, telles que la technique de floutage, qui ne sont pas requises aujourd'hui par la loi, peuvent être efficaces pour assurer préventivement le respect de la vie privée. En effet, il conviendrait de masquer les données personnelles, telles que des plaques d'immatriculation, des visages, des boîtes aux lettres, ou tout élément attribuable à une personne, lorsque ces données ne sont pas strictement nécessaires à la mission du drone.²⁸³ De la même manière, il serait intéressant d'explorer toutes ces mesures techniques de prévention tirées de la pratique pour les incorporer dans le régime légal applicable aux drones en Belgique.

²⁸² R. FINN, D. WRIGHT, L. JACQUES, P. DE HERT, *op. cit.*, p. 346.

²⁸³ Voy. Annexe 2, point 4.

CONCLUSION

Etant l'une des inventions les plus captivantes de l'homme ces dernières années, les drones sont généralement mal perçus par l'opinion publique. Toutefois, comme nous avons pu le constater dans la deuxième partie de ce travail, les drones ont des capacités multiples. En effet, les drones civils permettent d'aider divers secteurs commerciaux, de sécuriser nos rues, d'assurer une meilleure application de la loi, et de protéger notre planète. Mais récemment les drones sont aussi devenus le nouveau jouet en vogue. Cette utilisation à des fins de loisir est sans doute l'usage des drones qui est la plus préoccupante.

En effet, une attention particulière doit être portée sur les utilisateurs privés de drones qui bénéficient d'une exemption pour leur utilisation strictement personnelle et domestique. L'utilisation raisonnable et conforme à la loi par les particuliers est ainsi moins facilement contrôlable que celle des acteurs économiques, qui doivent être titulaires d'une licence. Les utilisateurs privés représentent dès lors un plus grand risque pour la sécurité et pour le droit à la vie privée.

Dans la première partie de ce travail, on découvre que la vie privée et le traitement de données sont relativement bien protégés tant au niveau européen qu'au niveau belge. Cependant, il est regrettable que la grande majorité des règles prévues en la matière ne permette qu'une protection curative et que les législations ne soient pas mieux adaptées aux fonctions multiples des drones.

On peut, toutefois, se réjouir de l'introduction, par la proposition de règlement, du principe de responsabilité et des différentes mesures tirées du *soft law* telles que le principe de *Privacy by Design*, les analyses d'impact et d'audit privée, qui vont favoriser l'adaptation et la mise en œuvre des règles de protection de la vie privée au domaine des drones. De même, l'adoption de cette proposition contribuera à développer les aspects préventifs de la protection de la vie privée. Finalement, la proposition de règlement assurera également un meilleur respect du principe de transparence qui est essentiel pour un processus démocratique. En effet, une

transparence accrue assurera une meilleure compréhension de l'utilité des drones et une plus grande acceptation de leur intégration au sein de la société.

Au regard des législations applicables en France et aux Etats-Unis, on observe que finalement ces deux pays, fervents utilisateurs de drones, ne sont pas d'avantage préparés à répondre aux questions de protection de la vie privée que peuvent soulever l'utilisation civile des drones. Il faut cependant souligner que la France a adopté deux arrêtés sur les drones qui règlent des questions de sécurité et un article pénal sanctionnant le non respect de l'image d'autrui existe dans son arsenal législatif. Par ailleurs, il est important de noter qu'aux USA, la protection de la vie privée par le biais du quatrième amendement de la Constitution est sacrée. La jurisprudence américaine en a fait une arme redoutable servant de garantie contre les ingérences excessives dans la vie privée des citoyens américains par les autorités étatiques, arme qui pourrait s'avérer efficace contre les drones.

L'adoption d'un arrêté royal en Belgique répondra à de nombreuses questions de sécurité posées par les drones. Toutefois, nous pensons qu'il n'apportera pas de nouvelles mesures en matière de vie privée. Puisque pour la protection de la vie privée, l'arrêté renvoie aux législations existantes, il est crucial de travailler à l'adaptation de ces lois à la technologie des drones. Des améliorations pourront déjà, en grande partie, être obtenues par l'adoption de la proposition de règlement. En effet, les aspects tirés du *soft law* constituent de réels renforcements pour la protection de la vie privée et facilitent l'ajustement des règles de vie privée. Insérer dans le cadre juridique des principes comme l'adoption de codes de conduites, le principe de *Privacy by Design*, les analyses d'impacts, et l'audit privé paraît donc essentiel. En outre, le principe de responsabilité prévu par le règlement, déplaçant la charge de la preuve sur le responsable du traitement est également une mesure préventive efficace car elle oblige le responsable de garantir et prouver, en amont, le respect de la vie privée pour chaque traitement de données.

L'individu choisissant de vivre en société doit accepter que certains aspects de sa vie privée fassent l'objet d'un traitement pour des fins légitimes. En effet, le traitement de données, selon les prescrits de la loi et nécessaire à des fins de surveillance, de sécurité, d'information, et de besoins économiques, justifie l'abandon

de certaines facettes de la vie privée. Les différents intérêts en présence doivent être mis en balance et un équilibre doit être trouvé entre la vie en société et la vie privée.

L'enjeu de l'intégration des drones dans l'espace aérien n'est aujourd'hui plus une question de légalité, surtout grâce à l'adoption de l'Arrêté royal. Le débat actuel est plutôt de comprendre quelle société veut se munir d'un outil efficace et profitable mais susceptible d'abus. Cette interrogation n'est pas récente mais s'est déjà posée avec l'introduction d'autres nouvelles technologies dans la société. Les citoyens exigent de l'Etat qu'il assure le respect de leurs droits et libertés mais en même temps ils demandent à leur gouvernement de garantir la sécurité et la croissance économique. Les citoyens attendent de l'Etat qu'il accomplisse l'exercice difficile de balancer les différents intérêts en présence et permette ainsi l'intégration, dans le respect de leurs droits, de ces nouvelles technologies assurant la sécurité et le développement économique. L'Etat doit veiller que ces évolutions technologiques apportées à la société ne violent pas les droits fondamentaux ; n'utilisent que les moyens les moins intrusifs ; s'introduisent dans le respect du cadre juridique déjà prévu pour d'autres technologies similaires ; et ne soient pas mises en œuvre sans protection adéquate.²⁸⁴

Soulignons que souvent, ce ne sont pas les drones en tant que tel qui suscitent des problèmes au niveau de la protection de la vie privée mais ce sont surtout les technologies, toujours plus développées et performantes, qui les équipent qui peuvent entraîner les questions de vie privée que nous avons identifiées.

Les drones représentent également un instrument précieux pour alimenter le *Big data*. Le concept de *Big data* constitue du matériau brut aux utilisations multiples. Par la collecte massive de données, le *Big data* permet aux entreprises et aux agents de l'Etat de comprendre et d'interpréter les comportements étudiés, qu'ils soient humains, économiques, sociaux, ou écologiques.²⁸⁵ Toutefois, le drone ne doit pas

²⁸⁴ P. ROSENZWEIG, S.P. BUCCI, C. D. STIMSON, ET J.J. CARAFANO, Backgrounder, « Drones in U.S. Airspace: Principles for Governance », *The Heritage Foundation*, 20 septembre 2012, n° 2732, pp. 4 et 5.

²⁸⁵ C. MIGLIETTI, « Big data, le matériau brut utile à tous les métiers », *Les Echos*, <http://www.lesechos.fr/idees-debats/cercle/cercle-130929-big-data-le-materiau-brut-utile-a-tous-les-metiers-1109382.php>.

devenir un outil corrompu qui rassemble systématiquement des vastes quantités d'informations allant au-delà de sa mission initiale.

ANNEXES

- ANNEXE 1 -

ENTREVUE AVEC PATRICK MASCART, VICE-PRESIDENT DE LA 'BELGIAN
UNMANNED AIRCRAFT SYSTEM ASSOCIATION', EN DATE DU LUNDI 11 MAI 2015

1. Dans quel secteur votre Association est-elle active ? Drones militaires ou civils ?

C'est uniquement les drones civils. Les membres sont autant des pilotes que des sociétés qui développent des applications ou du matériel technique.

2. Aujourd'hui pour faire voler un drone, faut-il une autorisation?

Seuls les vols qui sont autorisés par la DGTA peuvent avoir lieu. (Direction générale Transport aériens) Ce sont les vols techniques, les vols scientifiques, les vols de démonstration, et les vols sur les terrains d'aéromodélisme. Donc chaque vol est soumis à l'autorisation de la part de la DGTA. Il n'y a donc pas d'autres possibilités de vols légitimes.

3. Qu'entendez-vous par vol technique.

Par vol technique, on entend un vol testant du matériel en cours de développement, ce n'est bien sûr pas « j'achète une caméra Sony je la mets sur mon drone pour vérifier comment cela fonctionne ». Il faut vraiment avoir développé un produit que vous désirez tester.

4. Un code de pratiques, qui comprend des lignes directrices serait-il bénéfique pour le secteur du drone ? Prévoir des analyses d'impacts relatifs à la protection de donnée permettrait une meilleure application de la loi ?

Oui bien sûr, c'est ce qui est déjà mis en place dans certains pays européens. A chaque vol qui présenterait éventuellement des risques particuliers, le pilote est obligé de fournir un scénario pour remédier aux différents problèmes de sécurité.

En France et en l'Allemagne, il y a tout un dossier à fournir pour les prises de vue à risque. C'est plus pour le risque que la protection de la vie privée. La vie privée encore une fois, à mon avis, il n'y aura rien qui sera mis réellement en place. Chaque pays devrait définir dans quel cas il y a « atteinte à la vie privée ». Je filme le jardin de mon voisin et on voit une piscine qu'il n'a pas déclarée, même s'il y a plus tard une implication fiscale, il n'y aura pas de conséquence pour le pilote. Il faudra vraiment voir au cas par cas.

5. Que pensez-vous de l'obligation d'être titulaire d'une licence pour faire voler un drone, pensez-vous que c'est réalisable, surtout pour les particuliers ?

Les professionnels devront effectivement passer une licence, on ne sait pas encore quel type de licence. Il y aura une partie théorique et une partie pratique. Le particulier, lui sera limité à une altitude et donc lui n'aura pas besoin de licence. Par professionnel on entend une personne qui veut faire une utilisation commerciale de son drone.

6. Le vendeur de drone ne devra-t-il pas avoir de licence ?

Non, par contre toutes les machines qui sortiront de son magasin devront être certifiées par la DGTA.

7. Comment contrôler l'altitude de vol pour le particulier ?

Le contrôle sera difficile. Le précédent document de Madame Galant précisait que 30 mètres devait être la hauteur maximum pour les particuliers. Aujourd'hui seul un télémètre peut confirmer cette distance et il est très difficile de vérifier sans cet instrument. C'est un danger, on en a averti le cabinet de la ministre et le groupe de travail. On verra comment ils l'ont transcrit dans le projet d'arrêté royal et s'ils en ont seulement tenu compte, sinon cela va être très difficile. De plus, il faut aussi connaître

les zones contrôlées. Une personne qui n'est pas informée pourrait ignorer qu'il se trouve dans une zone contrôlée près d'un aéroport ou d'autres zones sous contrôle.

8. Existe-il d'autres solutions que la limite de l'altitude?

Pour éviter les dégâts, la solution principale consiste à limiter le poids des drones qui sont autorisés à la vente. Par exemple, les «Phantom 3 » qui permettent de voler dans un rayon de 800 mètres, posent problème. C'est comme les « Gopro » : au tout début on en voyait quelques-unes et puis tout le monde en a eu. Il n'y avait pas de cadre et les propriétaires filmaient un peu tout et n'importe quoi. C'est exactement la même chose avec les drones. Une fois que le cadre légal sera sorti, les gens risquent de se précipiter sur des machines qui vont leur permettre de voler à 800 mètres du point de décollage. Il est clair que si la personne n'est pas un peu sensée, il utilisera au maximum les possibilités du drone et c'est là qu'est le problème. Ce sont des drones en vente libre ; il faut que le ministère en soit conscient et il faut aussi que le ministère de l'économie se penche sur le problème et pas uniquement le ministère des transports. Par contre si on impose une limite au niveau du poids, un poids raisonnable, si on peut utiliser qu'un «Parrote » par exemple, cela va tout de suite calmer l'ardeur de certains. D'autres pays ont décidé de limiter le poids à un kilo, ou un kilo et demi. A ce moment-là si les gens veulent des machines plus puissantes et voler ou ils veulent ils doivent passer une licence.

Un groupe de travail sera mis en place normalement dès que l'Arrêté Royal sera envoyé aux régions. Notre commission espère participer à ce groupe de travail et pouvoir rectifier le tir.

9. Sera-t-il difficile de faire respecter la vie privée par les particuliers ? Est-ce que l'arrêté en tiendra compte ?

La Commission européenne a défini qu'il y avait pas lieu de faire des réglementations supplémentaires par rapport à la vie privée, que les différents pays européens ont déjà un cadre bien établi et donc qu'il faut suivre les règles en vigueur dans chaque pays. Il est clair qu'un professionnel ne va pas s'amuser à aller faire des vidéos d'une femme dans un jardin, il a autre chose à faire. La législation sur la vie privée est claire : dès qu'il y a atteinte à la personne et que le dommage est clairement établi, une sanction

suivra si une plainte a été déposée. C'est au législateur à définir quand la personne qui se sent lésée peut porter plainte. C'est à la justice de définir s'il y a un dommage à établir ou s'il y a une violation de la vie privée. Il faut voir l'utilisation qui est faite de l'image et il faut que la personne soit au courant, c'est la même chose pour le GSM. Il faudra voir comment la justice réagit mais il n'y aura pas de législation particulière liée aux drones, on renvoie à la loi sur la vie privée, il n'y a pas de loi supplémentaire.

10. Quand l'Arrêté royal sera t'il en application ?

Il devrait être écrit dans les jours qui viennent et être envoyé aux régions et ensuite au Conseil d'Etat. Il ne faut pas oublier que la Commission européenne a un droit de regard aussi sur cet arrêté. Mais il ne sera pas applicable avant la fin de l'année.

- ANNEXE 2 -

ENTREVUE AVEC GREG BILLEN, MANAGING PARTNER DE DMS (DRONE MEDIA SERVICE), EN DATE DU 13 MAI 2015

1. Dans quel secteur êtes-vous actif avec vos drones

Mon entreprise est membre de BEUAS. Drones Média Service (DMS) est actif dans le secteur des services. Nos services sont spécialisés dans la photo, la vidéo et l'inspection technique. Nous utilisons pour la photo des appareils de 36 millions de pixels, pour la vidéo du 4K. Pour l'inspection, en plus de la photo et de la vidéo, on utilise de l'infrarouge.

2. Avez-vous besoin d'une autorisation spécifique pour voler ?

Actuellement oui, il faut essayer de faire rentrer nos activités dans un des 4 cas d'autorisation possible. Nous avons travaillé pour la SNCB pour l'inspection de leurs caténaires, ce service nous l'avons fait rentrer dans les vols techniques, de même que pour l'inspection des éoliennes de ELIA. Tous les deux sont des tests facturables. Nous travaillons surtout à l'étranger pour rentabiliser notre travail, principalement au Luxembourg, vu qu'une loi existe dans ce pays et que les autorisations sont plus rapides. En France nous sommes moins actifs car la législation est très différente, il faut par exemple un parachute qui se déploie en cas de problème technique. Alors qu'en Belgique le parachute est interdit.

Il y a un problème de délai pour les demandes d'autorisation, en effet le délai d'attente est trop long. Dans l'autorisation il est demandé de respecter les cours pratiques et théoriques que les professionnels ont suivis. Il faut également avoir passé l'examen de ces cours pour obtenir une autorisation.

3. Que va prévoir la Belgique pour les scénarios catastrophes ?

Je crois que l'appareil va devoir être contrôlable encore avec un rotor hors service. Cependant il y aura probablement pour les zones à risques l'obligation de rester

contrôlable si deux rotors sont hors service. Les RPAS 4 rotors seraient interdits pour les professionnels, la police pourra ainsi aisément reconnaître la différence entre professionnels et particuliers. De plus les 4 rotors en cas de panne d'un rotor ne sont plus contrôlables. Je pense que tolérer les 4 rotors pour les professionnels soutiendrait le travail en noir, puisqu'il n'y aurait pas une claire démarcation entre les particuliers et les professionnels. La limite par ces rotors paraît bonne. Je pense qu'il y aura également une limitation de poids, qui serait d'un kilo pour les particuliers. C'est peu un kilo, un RPAS équipé avec une caméra et le matériel nécessaire dépasse certainement le kilo.

4. Que mettez-vous en œuvre pour respecter la vie privée ? Savez vous quels lois vous devez respecter ? Comment les appliquer ?

Nous devons respecter la loi caméra de 2007. Tout ce qui est identifiable doit être flouté ou masqué, ceci est fait en postproduction par notre infographiste. Il ne faut pas qu'on puisse lire une plaque d'immatriculation, identifier un visage, ou voir le numéro d'une boîte aux lettres par exemple. Nous essayons d'éviter de filmer autant que possible certains plans ou détails qu'on va devoir masquer. Notre intervenant le fait sans savoir exactement quelle loi l'impose mais ceci lui permet d'être sûr de respecter la loi en matière de vie privée. Il pense qu'on lui a dit cela au cours de la formation théorique qu'il a suivi. Ces formations sont données par Espace Drone, qui a également organisé le salon du drone en mars dernier. Espace Drones a donné ses cours de connivence avec la DGTA (Direction Générale de Transport Aérien), qui avait un droit de regard sur ces cours et pouvait modifier les contenus du cours. Il pense que c'est probablement la DGTA qui a imposé de flouter les images.

5. Serait-il bénéfique d'établir un code de pratique, qui comprendrait des lignes directrices pour le secteur ? Devrait-on prévoir des analyses d'impacts relatifs à la protection des données pour vous aider à appliquer la loi ?

Oui ce serait bénéfique ! Il y a eu des directives qui prévoyaient des guidelines, mais la ministre n'en a pas tenu compte.

6. *Pensez-vous qu'un règlement plutôt qu'une directive serait préférable pour légiférer la matière, car une directive ne fixe que les objectifs à atteindre alors que le règlement est contraignant et doit être mis en œuvre dans son intégralité.*

Au plus précis et sévères seront ces lignes directrices et le contrôle au mieux cela sera pour une reconnaissance du secteur.

7. *Que pensez-vous de l'altitude que prévoyait l'Arrêté royal ?*

Je pense que si on n'autorise pas aux hélicoptères d'aller en dessous de 200 mètres et qu'on augmente l'altitude limite des RPAS cela pourrait créer de l'emploi. Je pense que si l'Arrêté n'augmente pas à 150 mètres d'altitude pour les professionnels, la région flamande risque de mettre la pression pour que le Conseil d'Etat refuse l'Arrêté. En effet en Flandre, les ailes sont beaucoup utilisées, mais pour être efficaces elles ont besoin de 110 mètres d'altitude sinon elles doivent faire trop d'allers retours, pour quadriller une zone. La hauteur de 30 pieds (91 mètres) prévue par l'Arrêté n'est pas suffisante, je pense qu'il faudrait augmenter à une altitude comprise entre 110 et 200 mètres, 150 mètres paraît optimal pour la sécurité ainsi que pour l'efficacité de différents types d'utilisation de RPAS.

8. *Que pensez-vous de l'obligation d'être titulaire d'une licence pour voler avec un drone ?*

C'est une bonne chose, je suis totalement pour. Cette licence devrait comprendre des matières qu'on impose déjà à certaines licences, par exemple la licence d'ULM ou à la Private Pilot Licence (licence pour les avions privés). A mon avis pour les RPAS on va vers une licence de montgolfière, il faudra que le professionnel ait des connaissances : (i) météorologiques ; (ii) aérodynamiques ; (iii) des règles aéronautiques ; et (iv) des facteurs humains.

9. *Avez vous déjà eu des plaintes pour non respect de la vie privée ?*

9.1 Nous n'avons jamais eu de plaintes, mais durant un vol où des habitations étaient proches, un habitant voulait voir si nous avions une autorisation. Je suis content de voir que les gens réagissent et j'étais heureux de montrer l'autorisation.

9.2 Je voudrais encore mettre en avant que l'usage des RPAS va créer de l'emploi et également assurer une plus grande sécurité comparée aux hélicoptères. L'usage des drones est plus sécurisant pour les pilotes mais aussi pour les autres. Enfin écologiquement, les RPAS sont bien plus avantageux que les hélicoptères car les RPAS utilisent majoritairement des batteries lithium polymères.

9.3 J'aurais aimé qu'on impose un transpondeur, mais je pense que ce ne sera pas le cas, je le déplore. Un transpondeur permettrait de savoir qui est le pilote de chaque RPAS professionnel en l'air. Cela permettrait peut être d'aider à prévenir les risques terroristes. La tour de contrôle pourrait brouiller des zones pour prévenir ces risques, on pourrait le faire pour certains endroits importants comme le Parlement européen, la Commission européenne, les stades, les centrales nucléaires.

9.4 Dès que l'arrêté sera entré en application seulement 1/4 à 1/5 de la Belgique sera « sur volable » sans autorisation pour les professionnels possesseurs d'une licence ou le particulier respectant ses limites. Le reste sera des zones d'exclusion, aéroport (zones CRT), zones militaire, pour lesquels il faudra une autorisation au cas par cas. Le privé devra en tenir compte de ces zones.

9.5 Finalement je pense que chaque machine sera reliée à chaque pilote, seul le pilote relié à la machine pourra le piloter ce qui permettrait en cas de crache d'identifier le responsable.

BIBLIOGRAPHIE

Législation

Législation internationale

- Déclaration universelle des droits de l'homme, signé à Paris le 10 décembre 1948.

Législation européenne

- Charte des droits fondamentaux de l'Union européenne, *J.O.U.E.*, C.326, 26 octobre 2012.
- Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, signé à Rome le 4 novembre 1950.
- 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, *J.O.C.E.*, L.281, 23 novembre 1995.
- Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), *J.O.C.E.*, L.201, 31 juillet 2002.
- Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE, *J.O.U.E.*, L.105, 13 avril 2006.
- Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à

caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), 25 janvier 2012.

Législation française

- Article 226-1 du Code pénale.
- Articles L223-1 et L251-1 du Code de la sécurité intérieure.
- Ordonnance n°2011-1012 du 24 août 2011 relative aux communications électroniques.
- Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure.
- La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Législation belge

- La Constitution belge.
- Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993, modifié en dernier lieu par la loi du 18 mars 2014, *M.B.*, 28 mars 2014.
- Loi du 13 juin 2005 relatives aux communications électroniques, *M.B.*, 20 juin 2005, modifié en dernier lieu par la loi du 27 mars 2014, *M.B.*, 28 avril 2014.
- Loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, *M.B.*, 31 mai 2007, modifié en dernier lieu par la loi du 4 avril 2014, *M.B.*, 25 avril 2014.

Jurisprudence

Jurisprudence internationale

- C.J.C.E., 13 mai 2014 (Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González), C-131/12.
- Cour eur. D.H., Von Hannover c. Allemagne (n°2), 7 février 2012, Req. n° 40660/08 et 60641/08.
- Cour eur. D.H., Springer AG c. Allemagne, 7 février 2012, Req. n° 39954/08.
- Cour eur. D.H., Reklos et Davourlis c. Grèce, 15 janvier 2009, req. n° 1234/05.
- C.J.C.E., 16 décembre 2008, Tietosuojavaltuutettu contre Satakunnan Markkinapörssi Oy et Satamedia Oy, C-73/07, *Rev. C.J.C.E.*, p. I-09831.
- Cour eur. D.H., Leempoel et SA éd. Ciné-Revue c. Belgique, 9 novembre 2006, Req. n° 64772/01.
- Cour eur. D.H., Oneryildiz c. Turquie, 30 novembre 2004, Req. n° 48939/99.
- Cour eur. D.H., Von Hannover c. Allemagne, 24 juin 2004, Req. n° 59320/00.
- C.J.C.E., 6 novembre 2003, Bodil Linqvist, C-101/01, *Rev. C.J.C.E.*, p. I-12971.
- C.J.C.E., 20 mai 2003, Rechnungshof (C-465/00) contre Österreichischer Rundfunk et autres et Christa Neukomm (C-138/01) et Joseph Lauermann (C-139/01) contre Österreichischer Rundfunk, *Rec. C.J.C.E.*, p. I-04989.
- Cour eur. D.H., Peck c. Royaume-Uni, 28 janvier 2003, req. n° 44647/98.

- Cour eur. D.H., *Pretty c. Royaume Uni*, 29 avril 2002, Req. n° 2346/02.
- Cour eur. D.H, X, Y et Z c Royaume-Uni 22 avril 1997, Req. n° 21830/93.

Jurisprudence belge

- Gand 1^{er} ch., 21 février 2008, *A.M.*, 2008/4, p. 318.
- Bruxelles, 7 avril 2000, *J.T.*, 2001, p. 779.
- Civ. Paris, 6 janvier 1976, *J.T.*, 1976, p. 209.
- Civ. Bruxelles, 17 janvier 1975, *J.T.*, 1975, p. 441.
- Civ. Bruxelles, 7 juin 1974, *J.T.*, 1975, p.135.
- Bruxelles, 26 décembre 1888, *Pas.*, 1889, II, p. 94.

Jurisprudence américaine

- US Supreme Court, *United States v. Jones*, 565 U.S. (2012), <https://supreme.justia.com/cases/federal/us/565/10-1259/>.
- US Supreme Court, *Kyllo v. United States*, 533 U.S. 27 (2001), <https://supreme.justia.com/cases/federal/us/533/27/case.html>.
- US Supreme Court, *Florida v. Riley*, 488 U.S. 445 (1989), <https://supreme.justia.com/cases/federal/us/488/445/case.html>.
- US Supreme Court, *California v. Ciraolo*, 476 U.S. 207 (1986), <https://supreme.justia.com/cases/federal/us/476/207/>.

- US Supreme Court, *Dow Chemical Co. v. United States*, 476 U.S. 227 (1986), <https://supreme.justia.com/cases/federal/us/476/227/case.html>.

Doctrine

- AFP, « L'homme qui avait revendiqué l'attaque de Charlie Hebdo tué par drone », *La libre*, 7 mai 2015, <http://www.lalibre.be/actu/international/l-homme-qui-avait-revendique-l-attaque-de-charlie-hebdo-tue-par-un-drone-554bb7dd35704bb01c2e2022>.
- ATAS C. et DEGROOVER M., La pratique de la vidéosurveillance en Belgique : application et évaluation de la loi du 21 mars 2007, in dans La vidéosurveillance. Entre usages politiques et pratiques policières, sous la direction de DEVRESSE M-S ET PIERET J., avec la collaboration de BELLIS P. et NOLET L., Bruxelles, Politeia.
- BADKAR M, « China May Use Drones To Kill The Smog Problem », *Business Insider*, 5 mars 2014, <http://www.businessinsider.com/china-is-testing-smog-clearing-drones-2014-3>.
- BELGA, « Un drone a survolé la centrale nucléaire de Doel », *La libre*, 20 décembre 2014, <http://www.lalibre.be/economie/actualite/un-drone-a-survole-la-centrale-nucleaire-de-doel-54958a3c3570e9972507022f>.
- BENSOUSSAN A., « Accountability and Protection of Personal Data », <http://www.globalprivacybook.com/blog-european-union/306-accountability-and-protection-of-personal-data>.
- BOURDOUX G.L., Vidéosurveillance et police : quel(s) profit(s) pour la police ? Quel(s) coût(s) pour la société ?, dans La vidéosurveillance. Entre usages politiques et pratiques policières, sous la direction de M-S. DEVRESSE et J. PIERET, avec la collaboration DE P. BELLIS et L. NOLET.

- CLARKE R., « Privacy impact Assessments », 2015, <http://www.rogerclarke.com/DV/PIA.html>.
- DE SALLE M., Civ. Bruxelles, 7 juin 1974, *J.T.*, 1975, obs.
- DEL VECCHIO G., « Essai sur les principes généraux du droit », *Rev. crit. législ. jurisp.*, 1925.
- DIJON X., *Le sujet de droit en son corps*, Société d'études morales, sociales et juridiques, 1982, Namur.
- DOCQUIR B., *Le droit de la vie privée*, Bruxelles, Larcier, 2008.
- DOUTRELEPONT C., « l'introuvable droit à l'image », in *Mélanges offerts à Raymond Vander Elst*, Tome I, Nemesis.
- ESPACE DRONE, *Manuel théorique du pilote de RPAS*, 1^{er} édition, Belgique, 2014.
- FINGAS J., « Secom offers a privacy drones, serves as our eyes when we're away », *Engadget*, 27 décembre 2012, <http://www.engadget.com/2012/12/27/secom-offers-a-private-security-drone/>.
- FINN R., WRIGHT D., JACQUES L., DE HERT P., *Study on privacy, data protection and ethical risks in civil Remotely Piloted Aircraft Systems operations*, rapport finale, Bruxelles, Commission européenne, 2014.
- GALLAGHER S., « Almost orbital, solar-powered drone offered as "atmospheric satellite" », *Ars Technica*, 18 août 2013, <http://arstechnica.com/information-technology/2013/08/almost-orbital-solar-powered-drone-offered-as-atmospheric-satellite/>.

- GOBLET C., « Audit en matière de vie privée & de données à caractère personnel », 2015, http://www.lexconsult.pro/avocat_services/audit-de-conformite-legislation-vie-privee-et-donnees-a-caractere-personnel.php
- GRAS M.L., « The Legal Regulation of CCTV in Europe », *Surveillance and Society Review*, Vol. 2, No. 3, 2004, [http://www.surveillance-and-society.org/articles2\(2\)/regulation.pdf](http://www.surveillance-and-society.org/articles2(2)/regulation.pdf)
- ISGOUR M., *Le droit à l'image*, Bruxelles, Larcier, 2014.
- ISGOUR M., Civ. Gand (16^e ch.), 24 juin 2002, *A.M.*, 2002/3, p. 143, obs.
- ISGOUR M. ET VINÇOTTE B., *Le droit à l'image*, Bruxelles, Larcier, 1998.
- LEONARD T. ET POULLET Y., « la protection des données à caractère personnel en pleine (r)évolution », *J.T.*, 1999.
- LINDON R., Paris, 27 février 1974, D., 1974, jur., p. 530, obs.
- MATGEN J.C., *Le voyeurisme est-il condamnable en tant que tel?*, 7 mai 2015, <http://www.lalibre.be/actu/belgique/le-voyeurisme-est-il-condamnable-en-tant-que-tel-554b6b3235704bb01c2d9a53>.
- MIGLIETTI C., « Big data, le matériau brut utile à tous les métiers », *Les Echos*, <http://www.lesechos.fr/idees-debats/cercle/cercle-130929-big-data-le-materiau-brut-utile-a-tous-les-metiers-1109382.php>.
- MILQUET J., « La responsabilité aquilienne de la presse », *Ann. Dr.*, 1989.
- MOUFFE B., *Le droit à l'image*, Waterloo, Kluwer, 2013.
- PEREZ S. ET CONSTINE J., « Facebook Looking Into Buying Drone Maker Titan Aerospace », *Techcrunch.com*, 3 mars 2014,

<http://techcrunch.com/2014/03/03/facebook-in-talks-to-acquire-drone-maker-titan-aerospace/>.

- ROAGNA I., « La protection du droit au respect de la vie privée et familiale par la Convention européenne des droit de l’homme », *Séries des précis droits de l’homme du Conseil de l’Europe*, Conseil de l’Europe Strasbourg 2012.
- ROGERS S., *Drones by country : who has all the UAVs ?*, 3 août 2012, <http://www.theguardian.com/news/datablog/2012/aug/03/drone-stocks-by-country>.
- ROSENZWEIG P., BUCCI S.P., STIMSON C.D., ET CARAFANO J.J., Backgrounder, « Drones in U.S. Airspace: Principles for Governance », *The Hirtage Foundation*, 20 septembre 2012, n° 2732.
- SANZ D., *Drones: que dit la loi?*, 24 février 2015, le figaro, <http://www.lefigaro.fr/actualite-france/2015/02/24/01016-20150224ARTFIG00147-drones-que-dit-la-loi.php>.
- SNIDER A., « Drones fly into nascent civilian market ripe with energy, environmental applications », *E&E Publishing*, 25 février 2012.
- THOMPSON II R. M., *Drones in Domestic Surveillance Opérations: Fourth Amendment Implication and Legislative Response*, Congressional Research Service, Report for Congress, 2013, p. 4, <https://www.fas.org/sgp/crs/natsec/R42701.pdf>.
- VILLASENOR J., « Observations from above: Unmanned Aircraft Systems and Privacy », *Harvard Journal of Law & Public Policy*, Vol. 36 N° 2, 2012, http://www.harvard-jlpp.com/wp-content/uploads/2013/04/36_2_457_Villasenor.pdf.

- VINCENT C., « de drones d'engins, sans pilotes et sans limites », *les echos*, <http://www.lesechos.fr/enjeux/business-stories/lenjeu-du-mois/02148899682-de-drones-dengins-sans-pilote-et-sans-limites-1117327.php>.
- VOORHOOF D., Gand, 20 septembre 2006, *Juristenkrant*, 2006, n°139, p. 5, obs.
- WONG R., « The Future of privacy », *Computer Law and Security Review*, 2010, p.3, trouvé sur http://works.bepress.com/rebecca_wong/12/.
- WRIGHT D., FRIEDEWALD M., GUTWIRTH S., LANGHEINRICH M., MORDINI E., BELLANOVA R., DE HERT P., WHADWA K. ET BIGO D., « Sorting out smart surveillance », *Computer Law & Security Review*, Vol. 26, 2010, pp. 10 et 11, trouvé sur http://works.bepress.com/serge_gutwirth/69/.
- Auvsiadmin, 19 Mars 2015, CNET : UAS's, newest mission ? Disaster relief, <http://increasinghumanpotential.org/cnet-uass-newest-mission-disaster-relief/>.
- Communication de la Commission au Parlement européen et au Conseil, Une nouvelle ère de l'aviation. Ouvrir le marché de l'aviation à l'utilisation civil de systèmes d'aéronefs télépilotes, d'une manière sur et durable, COM (2014) 207 final, Bruxelles, 8 avril 2014.
- Commission de la protection de la vie privée, « Questions les plus fréquemment posées – Drones », FAQ 2014, <http://www.privacycommission.be/fr/faq-page/7346#t7346n16588>.
- Groupe de travail « Article 29 », Remotely Piloted Aircraft Systems (RPAS) – Response to the Questionnaire, European Commission, Bruxelles, Décembre 2013, trouvé sur http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20131216_reply_to_rpas_questionnaire.pdf.

- European RPAS Steering Group, *Roadmap for the intergation of civil Remotely-Piloted Aircraft Systems into the European Aviation System*, juin 2013.
- Conseil de l'Europe, Commission Staff working document Towards a European strategy for the development of civil applications of Remotely Piloted Aircraft Systems (RPAS), 13438/12, bruxelles, 6 septembre 2012.
- Groupe de travail « Article 29 », Opinion 3/2012 on developments in biometric technologies, 00720/12/EN WP193, Bruxelles, 27 avril 2012, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf.
- PIAF Project, *A Privacy Impact Assessment Framework*, 2012, <http://www.piafproject.eu>.
- Groupe de travail « Article 29 », Opinion 3/2010 on the principle of accountability, Bruxelles, 13 juillet 2010.
- Groupe de travail « Article 29 », Opinion 4/2007 on the concept of personal data, 01248/07/EN WP 136, Bruxelles, 20 juin 2007, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.
- Groupe de travail « Article 29 », Opinion 4/2004 on the processing of personal Data by means of Video Surveillance, 11750/02/EN, WP 89, Bruxelles, 11 février 2004, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp89_en.pdf.
- European Advisory Group on Aerospace, « STAR 21 : Strategic Aerospace Review for the 21st Century », Brussels, 2002.
- Commission de la protection de la vie privée, avis 14/95 du 7 juin 1995 sur Applicabilité de la loi du 8 décembre 1992 relative à la protection de la vie

privée à l'égard des traitements de données à caractère personnel à l'enregistrement d'images et ses conséquences, https://epic.org/privacy/surveillance/cbvp_vs_avis14_95_060795.pdf.

- Commission européenne, Flying new way - a boost for european creativity and innovation, http://ec.europa.eu/enterprise/flipbook/rpas/?goback=.gde_941207_member_238344699#/1/zoomed.
- AUVSI, « The Benefits of Unmanned Aircraft Systems : Saving Time, Saving Money, Saving Lives », *Association for Unmanned Vehicle Systems International (AUVSI)*, p. 2, <https://epic.org/events/UAS-Uses-Saving-Time-Saving-Money-Saving-Lives.pdf>.
- Adams technology Pvt. Ltd., « Battelfield Acoustics-Microflown », *Adams Technology*, <http://www.adams-tech.net/project/battlefield-acoustic-systems-microflown/>.
- Commission de la protection de la vie privée, loi vie privée, <http://www.privacycommission.be/fr/la-loi-vie-privee>.
- Farming Drones, UAVs in the Agriculture Industry, <http://farmingdrones.com>.

Place Montesquieu, 2 bte L2.07.01, 1348 Louvain-la-Neuve, Belgique www.uclouvain.be/drt

