IRIS Spécial

Publié par
l'Observatoire européen de l'audiovisuel

Smart TV et protection des données

OBSERVATOIRE EUROPÉEN DE L'AUDIOVISUEL

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

IRIS *Spécial*
Smart TV et protection des données

Observatoire européen de l'audiovisuel, Strasbourg 2016
ISBN 978-92-871-8238-8
EUR 49

Directeur de la publication – Susanne Nikoltchev
Directrice exécutive, Observatoire européen de l'audiovisuel

Contrôle éditorial – Maja Cappello
Responsable du département Informations Juridiques, Observatoire européen de l'audiovisuel

Equipe éditoriale – Francisco Javier Cabrera Blázquez, Maja Cappello, Sophie Valais
Observatoire européen de l'audiovisuel

Auteurs – Britt van Breda, Nico van Eijk, Kristina Irion, Tarlach McGonagle, Sander van Voorst
Institut du droit de l'information (IViR), Université d'Amsterdam

Assistant éditorial – Olivier Mabilat, Snezana Jacevski, Observatoire européen de l'audiovisuel

Commercialisation – Markus Booms, markus.booms@coe.int, Observatoire européen de l'audiovisuel

Presse et relations publiques – Alison Hindhaugh, alison.hindhaugh@coe.int, Observatoire européen de l'audiovisuel

Traducteurs / Relecteurs – Aurélie Courtinat, Johanna Fell, Julie Mamou, Maco Polo Traductions, Stefan Pooth, Roland Schmid, Sonja Schmidt, Lucy Turner, Anne-Lise Weidmann

Editeur
Observatoire européen de l'audiovisuel, 76, allée de la Robertsau F-67000 Strasbourg, France
Tél. : +33 (0)3 90 21 60 00, Fax : +33 (0)3 90 21 60 19
E-mail : info.obs@coe.int, www.obs.coe.int

Organisation partenaire ayant contribué à l'ouvrage
Institut du droit de l'information (IViR), Université d'Amsterdam, Vendelstraat 7, 1012 XX Amsterdam, Pays-Bas
Tél: +31 (0) 20 525 3406, Fax: +31 (0) 20 525 3033
E-mail : ivir@ivir.nl, www.ivir.nl

Photocomposition / Impression – P O I N T I L L É S, Hoenheim, France

Veuillez citer cette publication comme suit :
Cappello M. (éd.), *Smart TV et protection des données*, IRIS Spécial 2015-2, Observatoire européen de l'audiovisuel, Strasbourg, 2016

IViR

OBSERVATOIRE EUROPÉEN DE L'AUDIOVISUEL

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Une publication de l'Observatoire européen de l'audiovisuel

Smart TV
et protection des données

Britt van Breda

Nico van Eijk

Kristina Irion

Tarlach McGonagle

Sander van Voorst

OBSERVATOIRE EUROPÉEN DE L'AUDIOVISUEL

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Avant-propos

Un homme déambule dans un centre commercial. Ses yeux sont flashés par une multitude de caméras équipées de logiciels de reconnaissance oculaire et, dans les vitrines des différents magasins, des écrans diffusent instantanément à son passage des publicités qui lui sont spécifiquement destinées ...

Il s'agit là bien entendu d'une scène tirée d'un film de science-fiction, en l'occurrence *Minority Report* de Steven Spielberg. Cette situation n'est toutefois pas si éloignée de ce que la technologie est actuellement en mesure de nous proposer. A l'ère d'internet, des téléviseurs connectés et des « écrans secondaires », les possibilités d'obtenir, de manière licite ou illicite, des données à caractère personnel sur les utilisateurs de médias se sont multipliées de façon exponentielle. Ces données constituent une matière première particulièrement importante pour les annonceurs, puisqu'elles peuvent être utilisées pour offrir des publicités personnalisées sur des services en ligne et divers types de périphériques connectés. En outre, les données à caractère personnel obtenues par l'intermédiaire des moteurs de recherche, des médias sociaux et des appareils connectés peuvent servir à offrir à l'utilisateur d'un service en ligne un meilleur confort d'utilisation.

L'obtention et l'utilisation des données à caractère personnel par des tiers, qu'elles soient le fruit d'un choix volontaire ou de l'inadvertance des utilisateurs, peuvent cependant s'avérer particulièrement intrusives dans leur vie privée. Il existe par ailleurs des situations dans lesquelles les informations sur la vie d'un utilisateur vont bien au-delà de ce que l'intéressé est prêt à accepter de dévoiler.

Ce problème se pose tout particulièrement lorsque la consommation audiovisuelle s'effectue au moyen de la smart TV, qui est en passe de s'imposer comme un équipement incontournable de nos foyers. Au niveau mondial, le nombre de ces dispositifs a doublé entre 2011 et 2015 et leur taux de pénétration moyen atteindra bientôt la plupart des foyers européens.

Selon une définition très générale, on entend par smart TV un téléviseur qui offre de multiples possibilités de connexion, parmi lesquelles figure au moins une connexion à internet. Une fois connectés, ces appareils sont capables de recueillir une multitude d'informations sur leurs utilisateurs, y compris leur milieu social et leur profil financier, qui peuvent ainsi être utilisées pour influencer le comportement de l'utilisateur en ligne à des fins de commercialisation directe ou de profilage des utilisateurs pour des activités publicitaires. Leurs fonctions englobent la reconnaissance vocale et faciale, la détection de mouvement, la création d'un compte et bien d'autres fonctionnalités interactives.

Compte tenu de cette tendance constante à remplacer la radiodiffusion traditionnelle par une consommation interactive (et intelligente) non-linéaire de contenus audiovisuels, le recours à des outils capables d'assurer un équilibre adéquat entre la volonté des fournisseurs d'optimiser leurs offres et de recommander des produits ou services qui correspondent aux choix personnels des utilisateurs et le besoin accru de protéger les utilisateurs contre tout risque de réduction du choix proposé, de manque d'information et, dans les pires cas de figure, contre toute forme de manipulation revêt une importance croissante.

Le cadre réglementaire actuellement en vigueur dans ce domaine est particulièrement morcelé et repose sur une multitudes de sources : une réglementation spécifiquement applicable aux médias contenue dans la Directive Services de médias audiovisuels ; des dispositions spécifiques prévues dans le cadre réglementaire des communications électroniques, la Directive relative au commerce électronique et la Directive relative au respect de la vie privée ; des dispositions générales en matière de respect de la vie privée contenues dans la Directive relative à la protection des données et la réglementation générale applicable à la protection des données ; et, enfin, une réglementation générale qui, notamment, définit un cadre de protection des consommateurs et intègre la dimension des droits de l'homme.

Compte tenu de la multiplicité de ce cadre juridique, diverses nouvelles questions d'interprétation relatives au traitement des données à caractère personnel par les opérateurs de la smart TV se posent au niveau national. Le présent IRIS *Spécial*, dont la rédaction a été confiée à l'Institut du droit de l'information (IViR) de l'Université d'Amsterdam, nous offre un aperçu des spécificités des smart TVs par rapport aux autres formes de médias audiovisuels. Il examine en outre le cadre réglementaire qui leur est applicable, avant d'analyser quatre études de cas et d'engager une réflexion sur les réformes réglementaires en cours.

Les évolutions dont nous sommes déjà témoins, parmi lesquelles figurent par exemple les *Smart Homes* (maisons intelligentes) équipées de réfrigérateurs connectés et les *Smart Things* (objets intelligents) tels que les ceintures connectées destinées aux soins de santé, semblent en effet exiger l'adoption d'une démarche intégrée qui traite l'ensemble de ces questions de manière cohérente. Cette démarche s'impose également sur le plan institutionnel, dans la mesure où une coordination entre les différents acteurs publics s'avère sans doute plus indispensable plus que jamais. Ces questions sont notamment abordées par le nouveau Règlement général sur la protection des données pour lequel un accord a été conclu le 15 décembre 2015 entre le Conseil, le Parlement et la Commission[1].

Cette publication offre un premier aperçu de l'issue de ce long processus décisionnel, qui a débuté en 2012. L'élaboration de ce document a également contribué à la tenue d'un séminaire, organisé le 11 décembre 2015 à Strasbourg par l'Observatoire, sur le thème des zones grises entre la réglementation applicable aux médias et la protection des données («*The grey areas between media regulation and data protection*»[2]), à l'occasion duquel ont notamment été examiné les défis auxquels sont actuellement confrontées les diverses parties prenantes, c'est-à-dire les régulateurs des médias, les organismes de protection des données, les professionnels du secteur, les fournisseurs de services de médias et les consommateurs. Compte de l'importance de ces questions, il convient que l'ensemble des parties concernées soient en mesure d'agir en toute connaissance de cause ; les différents chapitres de cet IRIS *Spécial* visent précisément à passer en revue les principales questions relatives à la consommation interactive de contenus audiovisuels. Il s'agit là d'une première série d'informations essentielles, auxquelles nous ne manquerons pas d'ajouter ultérieurement des éléments supplémentaires.

Strasbourg, janvier 2016
Maja Cappello
Responsable du Département Informations juridiques
Observatoire européen de l'audiovisuel

[1] Voir http://www.consilium.europa.eu/fr/press/press-releases/2015/12/18-data-protection/.

[2] Voir http://www.obs.coe.int/workshops/-/asset_publisher/kNG5qM2wH8Kq/content/dli-workshop-obs-epra-the-grey-areas-between-media-regulation-and-data-protection.

Table des matières

Sigles et abréviations

API	Interface de programme d'application
CBP	College bescherming persoonsgegevens (Autorité néerlandaise de protection des données)
CCPA	*Cable Communications Policy Act* (loi américaine sur les communications par câble)
COPPA	*Children's Online Privacy Protection Act* (loi américaine sur la protection de la vie privée des enfants en ligne)
ECPA	*Electronic Communications Privacy Act* (loi américaine sur le respect de la vie privée en matière de communications électroniques)
EPG	Guide électronique de programmes
EPIC	Electronic Privacy Information Center
FTC	Federal Trade Commission
HbbTV	Hybrid Broadcast Broadband TV
IdO	Internet des objets
REC	Règles d'entreprise contraignantes
RGPD	Règlement général sur la protection des données
SMAV	Services de médias audiovisuels
WBP	*Wet bescherming persoonsgegevens* (loi néerlandaise sur la protection des données)

Introduction

Avec l'avènement d'une télévision interactive polymorphe, la réalité semble plus que jamais rattraper les prédictions cauchemardesques d'auteurs tels qu'Aldous Huxley, Ray Bradbury ou – le plus fameux d'entre eux – George Orwell. De nos jours, la technologie rendant possibles les sinistres « télécrans » de son roman *1984*, qui émettent et transmettent simultanément, peut être mise en veille, mais jamais complètement éteinte. Elle perçoit le moindre son « au-dessus d'un chuchotement très bas », capte tous les mouvements dans son champ de vision, est enfin largement disponible et amplement utilisée[3].

Certains types de téléviseurs (dits « intelligents » ou « smart TV ») sont à même de réagir à des stimuli visuels/gestuels et acoustiques (tels que la reconnaissance faciale ou celle des mouvements du corps et la reconnaissance vocale). Le fait que les smart TV puissent collecter, conserver et traiter des informations à caractère personnel fournies par leurs utilisateurs soulève une série de questions liées à la vie privée, auxquelles les cadres réglementaires régissant les médias audiovisuels traditionnels ne répondent pas. La présente étude[4] porte sur le rôle de la réglementation relative au respect de la vie privée dans le secteur des médias audiovisuels, en accordant une attention particulière aux téléviseurs intelligents ou smart TV.

Il fut un temps où la télévision était un appareil volumineux relégué dans un coin du salon, guère plus que « des fils et des lumières dans une boîte », pour citer la célèbre formule du journaliste Ed Murrow[5]. Les technologies et les marchés ont par la suite évolué pour aller vers des modèles plus maniables, plus légers et aux écrans plus plats, mais le principe de base demeurait : le téléviseur restait un appareil recevant des signaux de radiodiffusion et diffusant des émissions sur son écran. Ces signaux étaient envoyés de point à multipoint et le rapport entre les spectateurs et leur téléviseur était unidirectionnel. En conséquence, la vie privée des téléspectateurs n'avait aucune place dans le droit ou la politique des médias.

C'est tout récemment, avec le brusque essor des appareils interactifs qui ont bouleversé la relation entre téléspectateurs et téléviseurs en la rendant bidirectionnelle, que les questions de protection de la vie privée ont fait leur apparition parmi les préoccupations des législateurs et des décideurs en matière de droit des médias. Ce profond changement tient avant tout à l'existence de fonctions interactives sur ces téléviseurs, mais aussi à la sensibilisation – lente, mais inexorable – du grand public aux questions touchant à la vie privée, de manière générale.

« Téléviseur connecté », « téléviseur hybride » et « téléviseur intelligent » sont autant de termes, peu ou prou synonymes, employés pour décrire ces téléviseurs interactifs. Tous désignent pour l'essentiel des téléviseurs (ou des associations entre téléviseur et technologie similaire sous forme de récepteur numérique ou « *set top box* ») qui permettent de voir des programmes de

[3] Orwell G., *1984*, Gallimard, Paris, 1950, trad. Amélie Audiberti, p. 13.

[4] L'équipe tient à remercier Natali Helberger pour ses remarques judicieuses sur la version préliminaire de l'étude et Patrick Leerssen pour son aide précieuse à la traduction.

[5] Murrow E. R., discours « Wires and Lights in a Box » prononcé à la convention de la Radio Television News Directors Association, Chicago, 15 octobre 1958, www.rtdna.org/content/edward_r_murrow_s_1958_wires_lights_in_a_box_speech.

télévision linéaires tout en offrant une valeur ajoutée : la possibilité d'utiliser des services complémentaires accessibles grâce à une connexion internet. « Connecté » fait donc référence à cette connexion qui permet aux téléspectateurs (désormais plutôt appelés « utilisateurs ») de profiter de ces services annexes. « Hybride » évoque la nature « convergente » de la technologie : un hybride de téléviseur et d'ordinateur. « Intelligent », terme manifestement choisi pour sa valeur commerciale et marketing, entend distinguer ces appareils de leurs prédécesseurs moins intelligents. Nous utiliserons dans la présente étude le terme de « smart TV ».

Tant qu'il n'est pas connecté à internet ou que ses fonctionnalités additionnelles ne sont pas activées, une smart TV n'est à tous points de vue rien de plus qu'un téléviseur traditionnel, qui permet à l'utilisateur de visionner des programmes de façon linéaire. Ce n'est toutefois pas le but recherché, au vu de ses capacités technologiques supplémentaires. La smart TV permet d'accéder à toute une palette de services en ligne : navigation internet, vidéo à la demande, réseaux sociaux et applications. L'utilisateur peut non seulement voir des contenus, mais aussi réaliser des transactions.

Ian Walden et Lorna Woods ont très bien diagnostiqué les préoccupations relatives au respect de la vie privée qui découlent des nouvelles fonctionnalités des smart TVs. Ils soulignent que « le paysage actuel de la radiodiffusion génère deux inquiétudes liées au respect de la vie privée, dans deux domaines-clés » :

> *« la capacité accrue de suivre et de mesurer nos habitudes de consommation de programmes radiodiffusés, particulièrement précieuse à des fins de profilage et de marketing, ainsi que la possibilité de surveiller ou d'intercepter les contenus que nous visionnons*[6]*. »*

Viennent s'y ajouter des inquiétudes de même type concernant le suivi, la mesure et la surveillance de nos habitudes de consommation de l'information et des contenus non radiodiffusés à l'occasion des autres activités en ligne que nous menons grâce aux smart TVs. La capacité de ces derniers de collecter et de traiter des données à caractère personnel au moyen de fonctions variées, telles que la reconnaissance vocale et faciale, est elle aussi source de préoccupation. Le traitement de ce type d'informations entraîne généralement leur communication à différents tiers, ce qui complique encore la situation du point de vue du respect de la vie privée.

Plus globalement, l'« écosystème » de la télévision intelligente fait intervenir un certain nombre d'acteurs qui, d'une façon ou d'une autre, ont ainsi accès à des informations concernant la consommation par l'utilisateur de contenus de radiodiffusion et ses activités en ligne, ainsi qu'à ses données personnelles. Cet écosystème regroupe le fabricant de ces téléviseurs, les fournisseurs de services HbbTV (*Hybrid Broadcast Broadband TV*), les opérateurs de portails et de boutiques d'applications, ainsi que les fournisseurs d'applications et de services de recommandation[7]. Globalement, la télévision intelligente fait intervenir une chaîne de valeur beaucoup plus hétérogène que les services de télévision traditionnels, en raison du nombre de parties prenantes, mais aussi des questions complexes soulevées par les modes de distribution[8].

Le fait que tant d'acteurs différents soient parties prenantes fait redouter la « multiveillance », c'est-à-dire un phénomène de « surveillance non seulement par l'Etat, mais aussi par les entreprises, les professionnels du marketing et les participants aux réseaux sociaux[9] ». Là encore, comme le formulent Ian Walden et Lorna Woods : « Certains acteurs de la chaîne de distribution ont le pouvoir de surveiller la consommation par les spectateurs des contenus de

---

[6] Walden I. et Woods L., « Broadcasting Privacy », *Journal of Media Law,* 2011, 3(1), p. 117-141, p. 121.

[7] Düsseldorfer Kreis, *Orientierungshilfe zu den Datenschutzanforderungen an Smart-TV-Dienste*, lignes directrices adoptées les 15-16 septembre 2015, p. 9 et suivantes, https://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/OH_Smart_TV_v1.0.pdf.

[8] Nooren P., Leurdijk A. et van Eijk N., « Net neutrality and the value chain for video », *info*, 2012, vol. 14, n° 6, p. 45-58, http://www.ivir.nl/publicaties/download/511.

[9] Richards N., *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age*, Oxford University Press, New York, 2015, p. 5.

radiodiffusion et ces relations peuvent ne pas être transparentes, tout comme les engagements des différentes parties peuvent ne pas être clairs et connus, du moins du point de vue du téléspectateur[10]. »

Structure

La présente étude s'articule autour d'une série de questions :

- Qu'est-ce que la télévision intelligente ?
- Quelles sont ses caractéristiques en comparaison d'autres types de médias audiovisuels ?
- Quels cadres réglementaires régissent la télévision intelligente ?
- Que nous enseignent les études de cas nationales ?
- Quels sont les dangers liés à la collecte, à la conservation et au traitement d'informations privées relatives aux utilisateurs par des acteurs commerciaux ?
- Quelle est l'évolution à prévoir des cadres réglementaires concernés ?

Le **chapitre I** étudie les différentes terminologies et définitions employées pour parler de la « télévision intelligente » et replace celle-ci dans le contexte des autres types de médias audiovisuels (interactifs). Il identifie comme suit les principales caractéristiques des smart TVs (dans une optique de protection des données et de la vie privée) : reconnaissance vocale, détection du mouvement, reconnaissance faciale, fonctions interactives (par exemple au moyen d'applications et des réseaux sociaux) ou encore comptes d'utilisateurs intégrés (par exemple chez Samsung). Toutes ces fonctions facilitent la collecte, la conservation et le traitement des informations à caractère personnel par des acteurs commerciaux. Elles serviront de grands axes dans les chapitres qui suivent pour la présentation du cadre réglementaire applicable et les études de cas.

Le **chapitre II** retrace comment la réglementation sur les médias audiovisuels et celle qui concerne la protection de la vie privée et des données se sont traditionnellement développées indépendamment l'une de l'autre. La convergence, l'émergence et le développement des technologies intelligentes obligent les législateurs de ces deux domaines à communiquer et revoir leur approche réglementaire pour tenir compte de ces évolutions et trouver des solutions. Ce chapitre étudie le manque de pertinence de la Directive SMAV ; la pertinence limitée des directives « accès » et « cadre » ; celle, croissante, de la directive sur la protection des données et de la directive vie privée et communications électroniques, ainsi que les conséquences prévisibles du (projet de) règlement général sur la protection des données. Il détaille également l'importance du droit de la consommation et de la législation relative aux droits de l'homme.

A partir de l'analyse de ce cadre réglementaire complexe, le **chapitre III** offre un aperçu des modalités selon lesquelles les questions juridiques y afférentes se posent et sont résolues, concrètement, à l'échelon national. Ce chapitre est composé de quatre études de cas puisant dans les expériences allemande, néerlandaise (deux exemples) et américaine :

1) Allemagne : position conjointe, test technique des téléviseurs intelligents et lignes directrices ;

[10] Walden I. et Woods L., « Broadcasting Privacy », *op. cit.*, note de bas de page 6, p. 140.

2) Enquête de l'Autorité néerlandaise de protection des données concernant le traitement des données à caractère personnel par TP Vision Netherlands avec ou par l'intermédiaire du smart TV Philips ;
3) Enquête de l'Autorité néerlandaise de protection des données concernant le traitement des données à caractère personnel par Ziggo dans le cadre de services numériques interactifs ;
4) *EPIC (Electronic Privacy Information Center) c. Samsung* : plainte auprès de la Federal Trade Commission américaine concernant l'interception et l'enregistrement systématiques, par Samsung, de communications privées de consommateurs à leur domicile.

Chacune de ces études de cas comporte une analyse détaillée des questions juridiques qui se posent et de leurs répercussions à plus grande échelle pour l'approche réglementaire du pays en matière de télévision intelligente.

Dans la lignée du chapitre III, le **chapitre IV** mène une réflexion sur les évolutions réglementaires à venir (en particulier les répercussions probables du règlement général sur la protection des données, actuellement à l'état de projet). Il s'attache aux caractéristiques des smart TVs identifiées précédemment et aux conséquences négatives de la collecte, de la conservation et du traitement des données à caractère personnel que permettent ces fonctionnalités technologiques.

Une analyse finale vient clore l'étude.

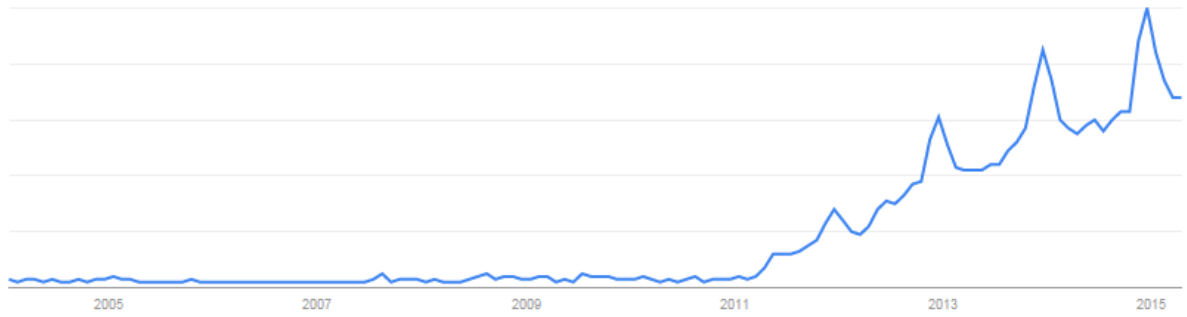
1. Définitions et caractéristiques

Les smart TVs connaissent un succès croissant dans les foyers européens, ce qui accroît en retour le degré de familiarité du grand public avec ces appareils. Le terme « télévision intelligente » (« *smart TV* » en anglais) évoque à juste titre celui de smartphone, même si ces équipements n'ont pas encore été adoptés aussi largement que leurs cousins téléphoniques.

1.1. Qu'est-ce qu'une smart TV ?

La popularisation du terme « *smart TV* » semble remonter à 2011, comme l'indique l'historique des recherches sur Google[11] (voir figure 1).

Figure 1 : Historique des recherches sur Google pour le terme « smart TV »



Source : Google trends

S'il n'a pas encore fait son entrée dans les dictionnaires, il est communément défini comme « un téléviseur capable de se connecter à internet ». D'autres définitions mettent l'accent sur la possibilité d'utiliser certaines applications, notamment fournies par des tiers[12].

La comparaison avec les téléviseurs ordinaires (« bêtes ») pourrait aussi fournir la base d'une définition élémentaire. Ces appareils-là consistent essentiellement en un écran. Tous leurs composants internes visent à afficher des contenus fournis par des sources externes telles que des antennes, des câbles, des prises péritel ou des connecteurs vidéo composites. Il en va de même pour les téléphones portables : les appareils ordinaires n'avaient pas d'autre fonction que la transmission de la voix par l'intermédiaire du réseau mobile. Les modèles plus sophistiqués étaient en mesure

[11] Graphique réalisé en ligne sur www.google.nl/trends.

[12] Kovach S., « What is a smart TV? », *Business Insider*, 8 décembre 2010, www.businessinsider.com/what-is-a-smart-tv-2010-12?IR=T.

d'établir une connexion internet rudimentaire par GPRS. Toutefois, ils ne pouvaient pas encore être qualifiés de smartphones.

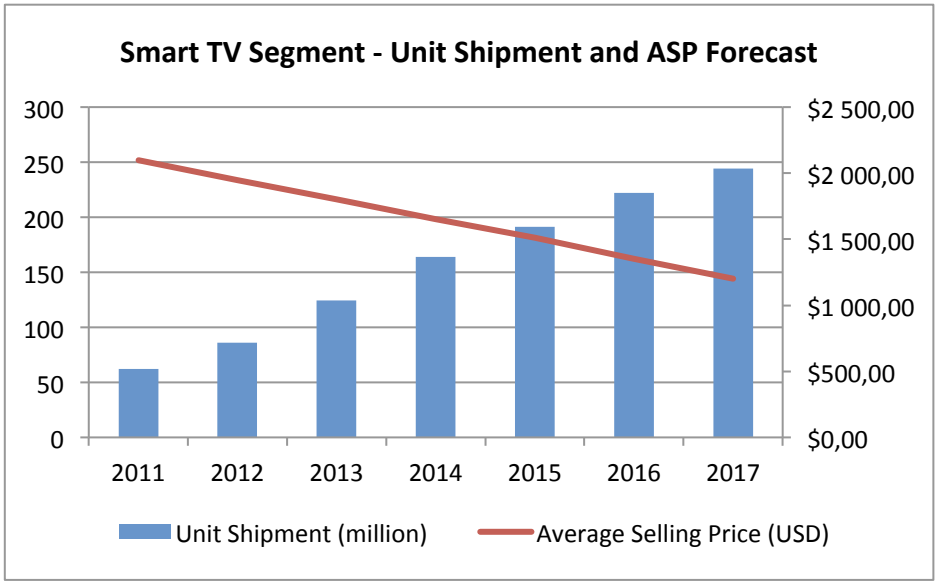
Comme leurs homologues « ordinaires », les smart TVs sont en mesure d'afficher des contenus par l'intermédiaire de toutes les sources susmentionnées. Ils offrent toutefois d'autres modes d'accès et sont ainsi pour la plupart compatibles Ethernet, wifi, USB et Bluetooth. Là encore, la comparaison avec les smartphones est parlante : ces canaux de communication permettent une connexion non seulement à des sources locales, situées à proximité immédiate de l'appareil, mais aussi à d'autres périphériques, quel que soit leur éloignement. Ces téléviseurs devraient en conséquence jouer à l'avenir un rôle important dans l'internet des objets (IdO).

Si l'on considère que la base de la définition réside dans la possibilité d'utiliser des applications, il faut souligner que les téléviseurs ordinaires sont également en mesure d'exécuter des programmes rudimentaires. L'élément distinctif des smart TVs réside dans leur système d'exploitation conçu pour servir de plateforme aux applications émanant de développeurs variés. En outre, ils possèdent généralement une certaine puissance de calcul qui leur permet d'exécuter des programmes bien plus complexes que les téléviseurs « bêtes » ordinaires. En somme, toute l'architecture de la smart TV repose sur cette fonction, qui s'ajoute à la diffusion d'images émanant de sources extérieures.

A la lumière de ce qui précède, nous proposons la description ou la définition suivante comme base de travail aux fins de la présente étude : « On entend par smart TV un téléviseur possédant de multiples possibilités de connexion, parmi lesquelles figure nécessairement une connexion internet. Il dispose en outre d'un système d'exploitation conçu pour fournir des contenus par l'intermédiaire d'applications, essentiellement via internet. L'appareil permet ainsi de visionner des programmes télévisés non linéaires et offre la possibilité à l'utilisateur d'accéder quand il le souhaite à des contenus qu'il a lui-même sélectionnés. »

On trouvera dans les tableaux qui suivent des précisions supplémentaires concernant la situation actuelle du marché et ses prévisions de croissance, en fonction de différents critères.

Figure 2 : Livraisons de smart TVs dans le monde 2011-2017

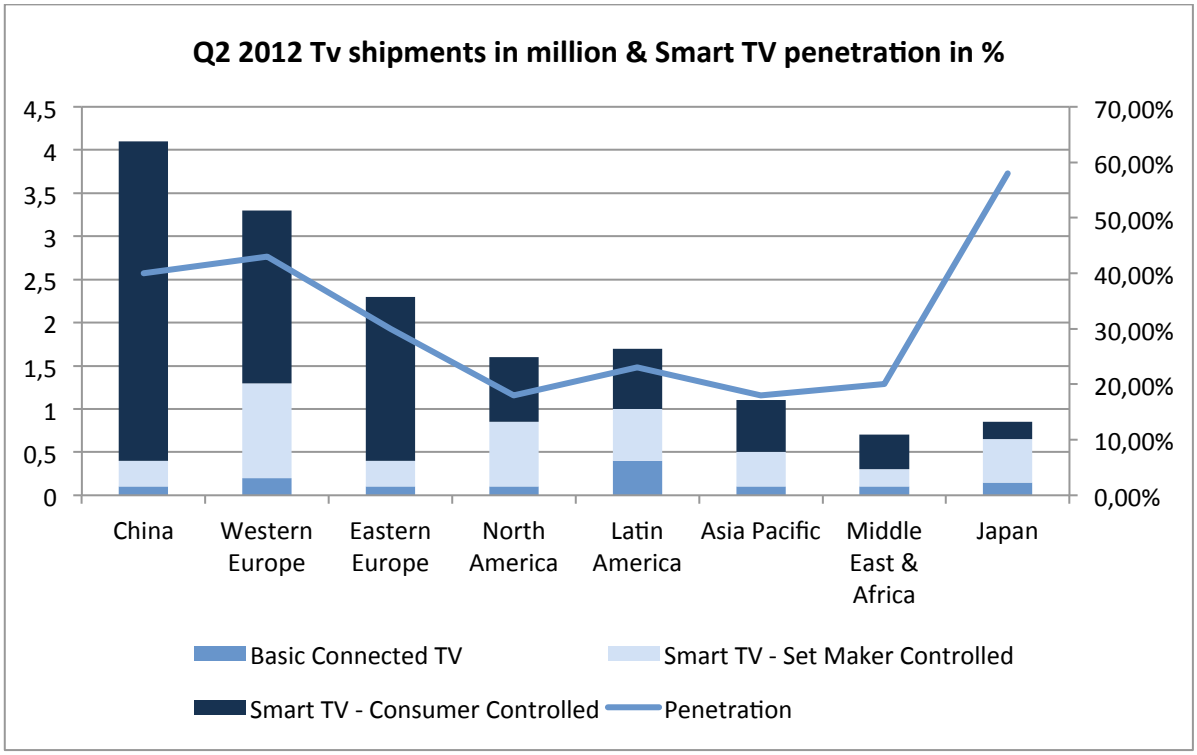


NB : tous les chiffres sont arrondis. L'année de référence est 2012.

Source : Frost & Sullivan

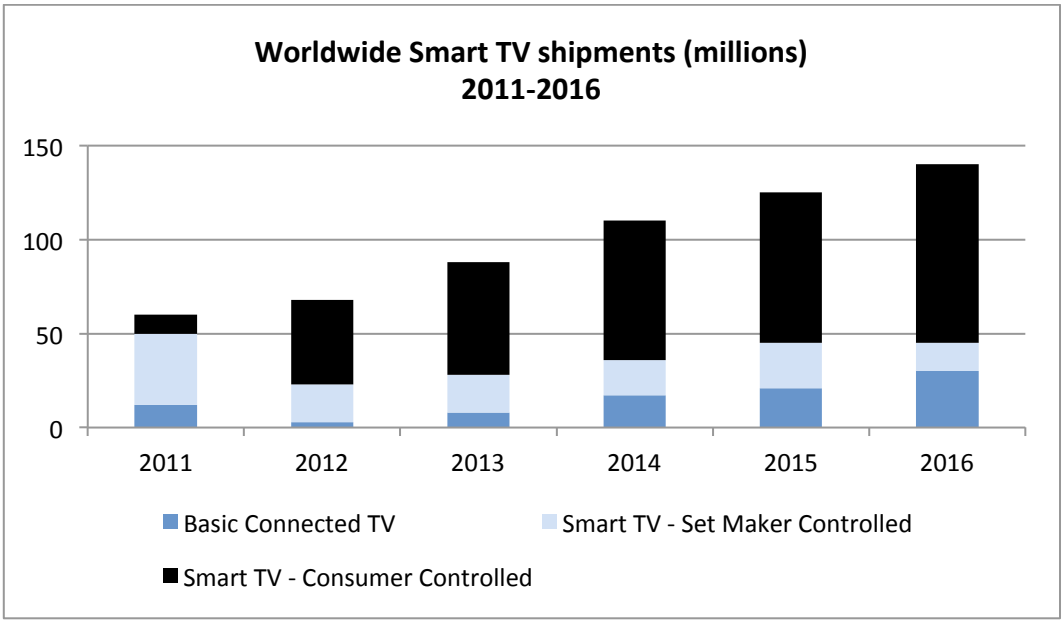
Ainsi que le montre la figure 2 à partir d'une autre source (Frost & Sullivan), les livraisons de smart TVs devraient connaître une hausse dans les années à venir et, comme c'est toujours le cas pour les « nouvelles » technologies, leur prix de vente moyen connaîtra une diminution continue.

Figure 3 : Livraisons de smart TVs par région au deuxième trimestre 2012 (en millions)



Source : NPD DisplaySearch Quarterly Smart TV Shipment and Forecast Report

Figure 4 : Livraisons de smart TVs – Prévisions 2011-2016



Source : NPD DisplaySearch Quarterly Smart TV Shipment and Forecast Report

Les figures 3 et 4 offrent un aperçu des modalités de contrôle de la connectivité internet des smart TVs. La tendance est nettement aux smart TVs équipés de navigateurs contrôlés par l'utilisateur. Les consommateurs souhaitent pouvoir naviguer à leur guise sur la Toile pour trouver des contenus (vidéo, généralement) correspondant à leurs goûts. Ceci est possible avec les smart TVs « contrôlés par le consommateur », tandis que les appareils « contrôlés par le fabricant » permettent uniquement au téléspectateur d'évoluer sur les plateformes conçues par ce même fabricant.

Tableau 1 : Parc mondial installé d'appareils de télévision connectée (en millions d'unités)

Classement au 2e trim. 2014	Fabricant	2e trim. 2014	2e trim. 2013	PDM 2e trim. 2014	Croissance du parc installé au 2e trim. 2014 (gliss. annuel)
1	Sony	123,8	96,8	24,8 %	27,9 %
2	Samsung	62,3	34,4	12,5 %	80,9 %
3	Nintendo	56,8	67,5	11,4 %	- 15,8 %
4	Microsoft	55,4	53,8	11,1 %	2,9 %
5	LG	32,2	16,0	6,5 %	101,9 %
6	Panasonic	29,9	19,6	6,0 %	52,4 %
7	Apple	18,7	13,0	3,8 %	44,7 %
8	Sharp	15,0	9,8	3,0 %	52,7 %
9	Toshiba	10,2	5,1	2,0 %	98,8 %
10	Philips	9,7	5,7	1,9 %	70,0 %
11	Roku	8,3	5,5	1,7 %	51,9 %
12	Google	6,0	0,0	1,2 %	sans objet

Note : l'expression « appareils de télévision connectée » recouvre les smart TVs, lecteurs de Blu-ray intelligents, consoles de jeu et lecteurs de médias en streaming.

Source : Gartner, Global Connected TV Device Tracker : Q2 2014

1.2. Quelles sont les informations collectées par une smart TV ?

A partir de cette définition opérationnelle des smart TVs, il est intéressant de présenter plus précisément les caractéristiques techniques de ces appareils (ou du moins de la majorité d'entre eux). Cette description se fonde sur un modèle standard[13] du constructeur Samsung, leader mondial sur ce segment avec une part de marché de 29 %[14]. L'appareil est équipé d'un « Smart Hub »,

[13] Il s'agit du modèle Samsung UE40F6320, qui présente la plupart des caractéristiques habituelles sur le marché à l'heure actuelle, voir www.samsung.com/uk/consumer/tv-audio-video/televisions/hd-tvs/UE40F6320AKXXU.

[14] IHS Technology, « TV Shipments Post Largest Annual Decline in Five Years, IHS Says », communiqué de presse, 10 septembre 2015, https://technology.ihs.com/548718/tv-shipments-post-largest-annual-decline-in-five-years-ihs-says.

passerelle au cœur de l'appareil qui permet d'accéder à de nombreuses applications et fonctions « intelligentes[15] ».

Les différentes fonctions proposées sont présentées dans le manuel d'utilisation. Un certain nombre d'entre elles sont recensées sous le titre « Interaction INTELLIGENTE », parmi lesquelles :

- la reconnaissance vocale ;
- la commande par mouvement ;
- la reconnaissance faciale ; et
- la création d'un compte Samsung.

Le téléviseur propose ainsi plusieurs modes de commande et offre la possibilité de créer un compte. Si ces fonctions améliorent sans aucun doute le confort de visionnage, elles appellent quelques mises en garde. Ainsi que nous l'avons mentionné plus haut, les téléviseurs traditionnels n'étaient guère plus que des écrans de visionnage. Avec leurs nouvelles fonctionnalités, les smart TVs doivent être équipés d'un certain nombre de capteurs qui sont « leurs yeux et leurs oreilles ».

Les pages qui suivent présentent ces capteurs et les données qu'ils sont susceptibles de collecter, un accent tout particulier étant mis sur les possibilités techniques offertes. Nous n'aborderons pas la question de savoir si cette collecte a effectivement lieu, point qui requerrait d'autres recherches d'envergure. Toutefois, des exemples concrets pourront être évoqués.

1.2.1. Reconnaissance vocale

Afin de pouvoir recevoir des commandes vocales, la smart TV doit être équipé d'un microphone capable d'enregistrer les sons aux abords de l'appareil. L'expression « reconnaissance vocale » indique que le téléviseur n'est pas seulement en mesure de capter des sons, mais aussi de filtrer ces données et de les traduire en commandes. En principe, il est donc envisageable que l'appareil stocke tous les mots prononcés à sa proximité et les passe au crible pour y détecter d'éventuelles commandes. Il ne s'agit pas seulement d'une hypothèse, comme en témoigne le tollé soulevé par les conditions d'utilisation des smart TVs de Samsung, qui ont fait la une des médias du monde entier avec cette clause :

> *« Veuillez noter que si vos paroles comportent des renseignements personnels ou d'autres informations sensibles, ceux-ci feront partie des données enregistrées et transmises à une tierce partie[16]. »*

Face à cette mauvaise publicité, Samsung a rapidement modifié le paragraphe mis en cause, mais cet incident montre que les smart TVs peuvent tout à fait enregistrer davantage d'informations que ne le pense l'utilisateur initialement. Du point de vue des annonceurs, la capacité d'entrer, au propre comme au figuré, dans des foyers privés ouvre d'innombrables possibilités de marketing. Nous étudierons ces questions de façon plus détaillée dans le chapitre III, avec l'étude de cas concernant la plainte déposée par l'Electronic Privacy Information Centre auprès de la Federal Trade Commission américaine.

---

[15] Voir le mode d'emploi du Samsung UE40F6320, *E-Manual*, 2013, http://downloadcenter.samsung.com/content/UM/201303/20130316094115068/%5BFRA%5DX12DVBEUF-0313.pdf.

[16] Harris S., « Your Samsung SmartTV Is Spying on You, Basically », *The Daily Beast*, 2 mai 2015, www.thedailybeast.com/articles/2015/02/05/your-samsung-smarttv-is-spying-on-you-basically.html#.

1.2.2. Commande par mouvement et reconnaissance faciale

Le téléviseur peut non seulement identifier des commandes vocales, mais aussi réagir aux gestes. Les utilisateurs peuvent en outre se connecter au Smart Hub à l'aide de la reconnaissance faciale.

Pour les besoins de ces fonctions, le téléviseur doit être équipé d'une caméra. Dans le cas du modèle qui nous occupe, une caméra externe a été ajoutée, mais de nombreux appareils comportent une caméra intégrée. Celle-ci permet au téléviseur d'enregistrer des images, par exemple en vue d'une conversation orale. Comme pour la reconnaissance vocale, on pourrait envisager un filtrage supplémentaire grâce auquel le logiciel identifierait et distinguerait les visages des différents utilisateurs. Ceci permettrait d'obtenir un aperçu du nombre de visionnages pour un contenu spécifique, mais aussi de l'identité des personnes concernées ou au moins de leurs profils d'utilisateur, sur la base de leurs habitudes de téléspectateur.

1.2.3. Compte (Samsung)

Cette rubrique regroupe d'autres données variées qui pourraient techniquement être collectées et donner lieu à la création de « profils » (délibérément ou non).

Les utilisateurs de smart TVs ont entre autres la possibilité de créer un compte auquel peuvent être rattachés divers types de données, telles que des suggestions ou recommandations de contenus en fonction du comportement du téléspectateur, mais aussi des publicités proposées sur le même principe ou selon les réactions de l'intéressé à de précédents messages publicitaires. Du point de vue des annonceurs, la création d'un compte par l'utilisateur lui-même est sans doute l'option la plus intéressante ; nous verrons plus loin pourquoi.

Même en l'absence de compte créé par l'utilisateur, des données sont toujours susceptibles d'être collectées. Comme c'est le cas avec d'autres appareils interconnectés, dès lors que le téléviseur est relié à internet, il est facile de créer un profil fondé sur les habitudes du téléspectateur et de le rattacher à l'adresse IP du téléviseur (laquelle permet également la localisation de ce dernier). Ces habitudes peuvent regrouper plusieurs éléments, tels que les contenus visionnés, l'identité du téléspectateur, ainsi que l'heure et la durée du visionnage (voir l'étude de cas allemande au chapitre III). Il est bien sûr possible d'éviter cela en omettant de connecter la smart TV à internet, ce qui réduit l'appareil, dans les faits, à un simple écran. Ce scénario est peu probable en raison de la variété et de l'attrait des fonctions « intelligentes ». L'analogie avec le smartphone coule de source : sans internet, il s'agit d'un simple téléphone dont bon nombre d'applications ne fonctionnent plus.

On peut conclure de ce qui précède qu'une smart TV se définit avant tout par sa connexion internet, la caractéristique qui en fait une composante de l'internet des objets. Un puissant processeur lui permet de plus d'exécuter différentes applications. Outre les caractéristiques énumérées dans la définition qui ouvre cette partie, la smart TV est aussi équipé d'un certain nombre de capteurs lui servant à observer ses alentours. Il est ainsi capable de collecter toutes sortes de données et potentiellement de les transmettre à l'autre bout de la planète via internet. Ces opérations pouvant se faire sans discernement, il s'ensuit que des données relatives à des mineurs ou à de simples visiteurs risquent aussi d'être enregistrées.

C'est parce qu'il intègre l'ensemble de ces fonctionnalités dans un appareil unique que la smart TV représente une étape importante dans l'évolution de la télévision intelligente et interactive. Ces fonctionnalités – lorsqu'elles existaient – étaient auparavant séparées et associées à des technologies distinctes, elles-mêmes régies par des réglementations différentes. Historiquement, l'une des raisons qui expliquent l'apparition de la réglementation relative aux médias a été l'influence de ceux-ci sur l'opinion publique. La portée et l'incidence des médias audiovisuels sont souvent rappelées dans ce contexte et la Cour suprême des Etats-Unis a elle-

même évoqué, dans un arrêt célèbre, « l'omniprésence singulière » du média télévisé, reconnaissable entre autres à sa capacité de pénétrer « dans l'intimité du foyer », où le droit de l'individu à ne pas être importuné est central[17]. Ce jugement a été formulé dans une affaire (*F.C.C. c. Pacifica*) portant sur la possibilité de laisser des images télédiffusées choquantes ou indécentes pénétrer dans le plus privé des espaces, le foyer familial. La technologie qui avait rendu possible cette intrusion, un simple téléviseur des années 1970, était unidirectionnelle. Les smart TVs relèvent d'une technologie tout autre. Leurs fonctionnalités bidirectionnelles éclairent sous un jour complètement nouveau « l'omniprésence singulière » de la télévision.

[17] Cour suprême des Etats-Unis, arrêt *Federal Communications Commission c. Pacifica Foundation*, 438 U.S. 726, 3 juillet 1978, p. 748, https://supreme.justia.com/cases/federal/us/438/726/case.html.

2. Cadres réglementaires

Les smart TVs constituent une nouvelle génération d'appareils convergents destinés aux utilisateurs finaux. A ce titre, leurs fonctions et les services auxquels ils facilitent l'accès relèvent de différents cadres sectoriels de l'Union européenne. Ces téléviseurs sont ainsi concernés par cinq ensembles de réglementation portant sur les médias audiovisuels, les communications électroniques, la protection des données, la protection des consommateurs et les droits de l'homme. Chaque instrument réglementaire poursuit un objectif unique et couvre différents aspects relatifs au fonctionnement des smart TVs. Pour les recenser, nous avons tenu compte de la façon dont ces appareils s'intègrent dans leur champ d'application respectif et des destinataires des obligations juridiques, parmi les acteurs de l'écosystème de la télévision intelligente[18].

A l'échelon de l'Union européenne, la répartition du travail de réglementation peut être résumée comme suit : la Directive Services de médias audiovisuels (SMAV) harmonise un ensemble minimal de dispositions relatives, selon le cas, aux services de médias audiovisuels linéaires ou à la demande[19] (« réglementation graduée »). Le cadre régissant les communications électroniques se compose de cinq directives concernant les réseaux et services de communications électroniques qui servent à l'acheminement des signaux, ainsi que les installations et services connexes, et certains aspects relatifs aux équipements terminaux. S'agissant des smart TVs, certaines dispositions de la directive « cadre[20] » et de la directive « accès[21] » s'appliquent, notamment en ce qui concerne les caractéristiques techniques des services de télévision numérique, telles que les interfaces de programmes d'applications (API), le système d'accès conditionnel et le guide électronique de programmes, autant d'éléments qui sont importants pour l'accès aux contenus et, en dernier ressort, la facilité à les trouver. L'accès aux services s'appuie sur la réglementation relative à la neutralité du réseau (dans la directive « service universel[22] »). La directive vie privée et

[18] Pour une étude plus générale de ces questions, voir Institut Hans Bredow pour la recherche sur les médias et Institut du droit de l'information, *HERMES – Study on the Future of European Audiovisual Regulation*, Hambourg/Amsterdam, octobre 2015, http://www.ivir.nl/publicaties/download/1643.

[19] Directive 2010/13/UE du Parlement européen et du Conseil du 10 mars 2010 visant à la coordination de certaines dispositions législatives, réglementaires et administratives des Etats membres relatives à la fourniture de services de médias audiovisuels (directive Services de médias audiovisuels), http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex:32010L0013.

[20] Directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive « cadre »), telle que modifiée par la directive 2009/140/CE et le règlement 544/2009, http://eur-lex.europa.eu/legal-content/FR/TXT/?qid=1446762384694&uri=CELEX:02002L0021-20091219 (version consolidée non officielle).

[21] Directive 2002/19/CE du Parlement européen et du Conseil du 7 mars 2002 relative à l'accès aux réseaux de communications électroniques et aux ressources associées, ainsi qu'à leur interconnexion (directive « accès »), telle que modifiée par la directive 2009/140/CE, http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:02002L0019-20091219 (version consolidée non officielle).

[22] Directive 2002/22/CE du Parlement européen et du Conseil du 7 mars 2002 concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques (directive « service universel »), telle que modifiée par la directive 2009/136/CE, http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:02002L0022-20091219 (version consolidée non officielle).

communications électroniques[23], qui fait également partie du cadre relatif aux communications électroniques, instaure des règles harmonisées en matière de droit à la vie privée, en ce qui concerne le traitement des données à caractère personnel dans le secteur des communications électroniques. Elle précise et complète la directive sur la protection des données[24] qui concerne le traitement des données à caractère personnel en général. Il convient également d'évoquer certaines composantes de la directive sur le commerce électronique[25] et de la législation de l'Union sur la protection du consommateur, telles que les règles relatives aux contrats conclus avec les consommateurs en matière de contenus numériques. Enfin, nous soulignerons aussi l'importance des textes relatifs aux droits de l'homme.

Malgré cette répartition des tâches, la situation pose quelques difficultés – comme nous allons le voir – tant ces cadres réglementaires se sont historiquement développés indépendamment les uns des autres. S'ils peuvent s'appliquer conjointement aux smart TVs, ils ne tiennent pas pleinement compte des objectifs des autres textes et ne se renforcent pas réciproquement de façon optimale. Qui plus est, les compétences en matière de surveillance réglementaire et d'application dans les Etats membres de l'Union sont elles aussi réparties entre plusieurs autorités, chacune chargée de mettre en œuvre la réglementation propre à son domaine. A quelques exceptions notables, les échanges d'informations et la coordination intersectorielle sont rares entre les autorités nationales, ce qui peut entraîner une efficacité moindre dans la réponse aux défis transversaux que posent les smart TVs.

2.1. Directive Services de médias audiovisuels

La Directive SMAV se trouve actuellement au cœur de la réglementation européenne concernant le secteur des médias audiovisuels[26]. Elle a succédé à la Directive Télévision sans frontières de 1989, précisément en réponse à la convergence des médias et aux transformations dans la production, les formats et la diffusion des médias. Cette notion nouvelle de « service de médias audiovisuels » (article 1, paragraphe 1, point a)) recouvre les formats télévisés bien connus, mais aussi les offres à la demande dans le cadre de médiathèques de contenus. Bien que les smart TVs puissent faciliter l'accès aux services de médias audiovisuels (sans parler des services en ligne, plus généralement), la Directive SMAV n'a pas vocation à s'appliquer aux équipements des consommateurs à proprement parler[27]. Les fabricants de smart TVs ne correspondent pas à la définition et se trouvent donc hors du périmètre de la réglementation. Les plateformes numériques exploitées par l'intermédiaire des smart TVs ne sont pas à proprement parler exclues du champ d'application de la directive, dans la mesure où elles proposent des services de médias audiovisuels. Les opérateurs intégrés verticalement qui commercialisent à la fois des appareils et un accès à des services de médias audiovisuels sont nombreux sur le marché de la télévision à péage. Ils relèvent en conséquence du

[23] 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), telle que modifiée par les directives 2006/24/CE et 2009/136/CE,

http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:02002L0058-20091219 (version consolidée non officielle).

[24] 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,

http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex:31995L0046.

[25] Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique »), http://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:32000L0031.

[26] Directive SMAV, *op. cit.*, note de bas de page 19.

[27] Les normes techniques et l'interopérabilité ne relèvent pas du champ de la Directive SMAV.

champ d'application de la Directive SMAV. Ces cas d'intégration verticale ne sont toutefois pas la norme sur le marché des smart TVs, où les fabricants d'appareils ne sont, traditionnellement, pas des producteurs de contenus.

Cependant, l'écosystème de la télévision intelligente englobe également les fournisseurs de services de médias audiovisuels tels que les chaînes de télévision et les catalogues de services de médias audiovisuels, dont la réglementation relève des lois des différents Etats membres de l'Union, conformément aux dispositions de la Directive SMAV. Avec les smart TVs, la mise en œuvre de la directive peut entraîner l'application d'exigences réglementaires différentes selon que les contenus de médias audiovisuels considérés sont linéaires ou non linéaires, alors qu'ils sont diffusés via le même écran[28]. La résolution du Parlement européen sur la télévision connectée fait observer à ce sujet que « la réglementation graduée, sous sa forme actuelle qui opère une distinction entre la radiodiffusion télévisuelle […] et les services audiovisuels à la demande, pourrait perdre de son importance, bien que des services d'informations et de communications faisant l'objet de réglementations différentes […] soient disponibles sur un seul et même appareil[29] ».

Dans la plupart des cas, la smart TV est le socle matériel d'une plateforme numérique qui connecte des tiers (fournisseurs de services de médias audiovisuels et autres services et contenus internet) avec sa base d'utilisateurs, grâce à une interface de programme d'application et une boutique d'applications affiliée. Ses fournisseurs, en tant que plateformes numériques, se trouvent cependant exclus du champ d'application de la Directive SMAV à l'heure actuelle. Pour illustrer les limites de la directive, prenons l'exemple des « *overlay ads* » (publicités en surimpression) grâce auxquelles le fournisseur de la plateforme numérique intègre ses propres formats publicitaires sur les smart TVs[30]. Dans la mesure où le fournisseur de plateforme numérique ne propose pas lui-même de services de médias audiovisuels, cette nouvelle forme de publicité n'entre actuellement pas dans le champ d'application de la Directive SMAV, même dans le cas de publicités en surimpression diffusées en lien avec des contenus audiovisuels émanant de fournisseurs tiers. La résolution du Parlement européen sur la télévision hybride conclut que les dispositions actuelles de la Directive SMAV « ne reflètent pas encore la fusion technologique croissante » et évoque la nécessité d'« [élargir] la notion de plateforme » lors de la révision à venir de la directive et de la réglementation connexe, en particulier le paquet « télécommunications »[31].

2.2. Cadre relatif aux communications électroniques

Le cadre réglementaire relatif aux communications électroniques s'applique avant tout à l'échelon des infrastructures et des transmissions. Il ne concerne pas la fourniture de contenus, l'exercice du contrôle éditorial sur ceux-ci ou encore les services de la société de l'information qui ne consistent pas entièrement ou principalement en la transmission de signaux sur les réseaux de communications

[28] Cf. Wagner C., « Connected TV: A challenge for market players and regulators », *Global Media & Communications Quarterly,* printemps 2012,

www.hoganlovells.com/files/Publication/41c5d3e3-0a16-4784-80c0-09193994456c/Presentation/PublicationAttachment/5fc8d47d-18e7-499a-8231-3b61f5067100/GMC_Quarterly_Summer_2012_v2.pdf ; Commission européenne, Livre vert « Se préparer à un monde audiovisuel totalement convergent : croissance, création et valeurs », COM(2013) 231,

http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=COM:2013:0231:FIN.

[29] Résolution du Parlement européen du 4 juillet 2013 sur la télévision hybride (télévision connectée), 2012/2300(INI), www.europarl.europa.eu/sides/getDoc.do?type=TA&language=FR&reference=P7-TA-2013-329.

[30] Commission européenne, *op. cit.*, note de bas de page 28.

[31] Parlement européen, *op. cit.*, note de bas de page 29.

électroniques[32]. Depuis les réformes de 2002, le champ d'application du cadre relatif aux communications électroniques est technologiquement neutre et englobe expressément les réseaux de radiodiffusion et les services de transmission, ainsi que les équipements utilisateurs pour la télévision numérique[33]. Désormais, les directives « cadre » et « accès » comportent de nouvelles règles concernant les services de télévision numérique qui sont d'une pertinence toute particulière pour les smart TVs. Cette évolution souligne l'importance croissante de la technologie sous-jacente aux services de télévision numérique. Les paragraphes qui suivent sont axés sur la réglementation de ces services et des services annexes dans le contexte de la télévision intelligente.

L'instrument central du cadre réglementaire relatif aux communications électroniques est la directive « cadre », qui comporte des définitions importantes. Les smart TVs répondent sans aucun doute à la définition de l'« équipement de télévision numérique avancée » présentée à l'article 2, point o), de la directive, qui couvre entre autres « tout poste de télévision numérique à décodeur intégré destiné à la réception de services de télévision numérique interactive ». Les plateformes numériques tournant sur des smart TVs comportent habituellement une interface de programme d'application (API) et des guides électroniques de programmes (EPG), ainsi qu'un système d'accès conditionnel. Les systèmes d'accès conditionnel et les EPG sont tous deux mentionnés dans l'article 2, point e *bis* comme des catégories de « services associés ». On trouve en outre la définition du « système d'accès conditionnel » (article 2, point f)) et de l'« interface de programme d'application (API) » (article 2, point p)). La directive « cadre » proprement dite réglemente les API, tandis que les dispositions relatives aux systèmes d'accès conditionnels et aux EPG se trouvent dans la directive « accès ».

L'API est un élément essentiel pour l'interopérabilité entre les applications des radiodiffuseurs ou des fournisseurs de services et les ressources des équipements de télévision numérique avancée, en l'occurrence les smart TVs. L'article 18 de la directive « cadre » exige des Etats membres qu'ils encouragent l'utilisation d'API ouvertes dans les services et équipements de télévision numérique interactive, afin de promouvoir l'interopérabilité de ces services. Cette injonction s'adresse en particulier aux « fournisseurs d'équipements de télévision numérique avancée mis en place pour recevoir des services de télévision numérique interactive sur des plates-formes de télévision numérique interactive » (article 18, paragraphe 1, point b)). Les propriétaires d'API sont encouragés à rendre « accessibles à des conditions équitables, raisonnables et non discriminatoires et moyennant une rémunération appropriée, toutes les informations nécessaires pour permettre aux fournisseurs de services de télévision numérique interactive de fournir tous les services reposant sur l'API, dans toutes leurs fonctionnalités » (article 18, paragraphe 2). Toutefois, du fait que la responsabilité en incombe aux Etats membres, les conséquences réglementaires sont moins strictes que ne seraient celles d'une obligation.

Aux termes de l'article 2, point f, de la directive « cadre », on entend par « système d'accès conditionnel » « toute mesure et/ou disposition techniques subordonnant l'accès sous une forme intelligible à un service protégé de radio ou de télévision à un abonnement ou à une autre forme d'autorisation individuelle préalable ». Cette définition recouvre les smart TVs permettant un accès conditionnel à des services de télédiffusion protégés (télévision à péage, par exemple) ; toutefois, elle ne s'applique pas à certains autres contenus protégés tels que les services de médias audiovisuels non linéaires ou les autres services en ligne. Au vu des fonctionnalités combinées des smart TVs, « la distinction […] peut être délicate et inapplicable[34] ». En conséquence, l'article 6, paragraphe 1, de la directive « accès » reprend les conditions énumérées dans son annexe I,

[32] Directive « cadre », *op. cit.*, note de bas de page 20, article 2, point c), et considérants 5 et 10.

[33] *Ibid.*, considérant 8.

[34] Helberger N., « Access to Technical Facilities in Digital Broadcasting », in : Castendyk O., Dommering E. et Scheuer A., *European media law,* Wolters Kluwer, Alphen aan den Rijn, 2008, p. 1129-1150, p. 1135.

première partie, concernant les systèmes d'accès conditionnel, mais limite leur application aux services de radiodiffusion protégés. Cette exigence oblige notamment les opérateurs de services à système d'accès conditionnel à en permettre l'accès aux radiodiffuseurs à des conditions équitables, raisonnables et non discriminatoires. De la même façon, les propriétaires de ces services doivent eux aussi respecter ces conditions lorsqu'ils octroient des licences aux fabricants de matériel grand public.

Les autorités réglementaires nationales ont le pouvoir d'imposer des obligations similaires, en matière d'accès, aux fournisseurs d'API et d'EPG, afin de garantir l'accès des utilisateurs finaux aux services de radio et télévision numérique (article 5, paragraphe 1, point b), en lien avec l'annexe I, deuxième partie, de la directive « accès »). De plus, ces autorités peuvent « imposer des obligations en rapport avec la présentation des guides électroniques de programmes et des outils de présentation et de navigation similaires » (article 6, paragraphe 4, de la directive « accès »). Toutefois, les constructeurs de smart TVs et les plateformes numériques associées ne sont soumis à aucune obligation de diffuser (« *must-carry* ») pour la transmission au public de chaînes de radio et de télévision particulières ou de certains services (article 31, paragraphe 1, de la directive « service universel »). Cette obligation est expressément adressée aux entreprises fournissant des réseaux de communications électroniques utilisés pour la diffusion de chaînes de radio et de télévision au public.

Hors du champ limité des exigences portant sur les services à accès conditionnel, les API et les EPG liés à des services de radio et de télévision numériques, le cadre relatif aux communications électroniques ne comporte aucune obligation générale concernant la neutralité et l'accès à des conditions équitables, raisonnables et non discriminatoires[35] qui s'appliquerait aux smart TVs et aux plateformes numériques connexes. Dans son Livre vert sur la convergence des médias, la Commission européenne souligne que l'abondance de contenus en ligne risque de limiter la découverte par les utilisateurs de contenus d'intérêt général pour des raisons variées telles que les mécanismes de filtrage et de personnalisation excessifs, les décisions économiques des fabricants d'équipements[36], etc. La résolution du Parlement européen sur la télévision hybride plaide, elle, pour l'instauration de « dispositions sur la possibilité de trouver les contenus et l'accès non discriminatoire aux plateformes, tant pour les fournisseurs et créateurs de contenus que pour les utilisateurs[37] ».

La technologie internet (« *back-channel* » ou canal retour) qui rend possibles les services interactifs de télévision intelligente est également soumise aux dispositions concernant la neutralité du net contenues dans le cadre relatif aux communications électroniques. La directive « cadre » dispose dans son article 8, paragraphe 4, que les Etats membres doivent favoriser « la capacité des utilisateurs finals à accéder à l'information et à en diffuser, ainsi qu'à utiliser des applications et des services de leur choix ». Cette disposition est précisée dans la directive « service universel » qui préconise la transparence et donne la possibilité aux législateurs d'intervenir. En vertu de cette obligation de transparence, les utilisateurs doivent se voir fournir des informations concernant toute procédure mise en place par l'entreprise pour mesurer et orienter le trafic de manière à éviter de saturer ou sursaturer une ligne de réseau, ainsi que des informations sur la manière dont ces procédures pourraient se répercuter sur la qualité du service. Les autorités réglementaires sont autorisées à imposer des exigences minimales en matière de qualité de service à une entreprise ou à des entreprises fournissant des réseaux de communications publics afin de prévenir la dégradation du service et l'obstruction ou le ralentissement du trafic sur les réseaux. Ce cadre relatif à la

[35] En anglais « FRAND » pour « Fair, Reasonable and Non-Discriminatory ». Il s'agit d'un critère fréquemment utilisé dans la réglementation sur les télécommunications.

[36] Commission européenne, *op. cit.*, note de bas de page 28.

[37] Parlement européen, *op. cit.*, note de bas de page 29.

neutralité d'internet est en cours de révision. De nouvelles dispositions devraient permettre le traitement prioritaire des services dits « spécialisés » et la fourniture de services gratuits (« taux zéro ») sera facilitée[38].

2.3. Réglementation sur le respect de la vie privée et la protection des données

Cette partie aborde l'importance croissante du cadre européen relatif à la protection des données pour l'écosystème de la télévision intelligente. Rappelons qu'en 2000, les institutions de l'Union ont officiellement adopté la Charte des droits fondamentaux, qui a acquis une valeur juridiquement contraignante en 2009 avec l'entrée en vigueur du traité de Lisbonne[39]. La charte codifie les droits fondamentaux des citoyens de l'Union concernant le respect de la vie privée (article 7) et la protection des données à caractère personnel (article 8).

Dans son Livre vert « Se préparer à un monde audiovisuel totalement convergent : croissance, création et valeurs », la Commission européenne rappelle que « traiter des données à caractère personnel est souvent la condition préalable au fonctionnement de nouveaux services, même si la personne n'est pas toujours bien informée de la collecte et du traitement de ces données[40] ». La personnalisation des contenus, dans certains cas comme celui des EPG ou d'autres services proposés sur certains portails, « peut être profitable aux consommateurs et annonceurs, mais elle dépend parfois d'outils posant des problèmes en matière de protection des données personnelles[41] ». Dans l'écosystème de la télévision intelligente, les données personnelles de l'utilisateur sont acheminées non seulement jusqu'au constructeur du matériel, au fournisseur de plateforme numérique et aux fournisseurs de services de médias audiovisuels (chaînes de télévision et médiathèques de contenus numériques), mais aussi aux fournisseurs de services en ligne. Le traitement des données à caractère personnel doit toutefois respecter la législation de l'Etat membre compétent, conformément au cadre de l'Union relatif à la protection des données.

Si la directive vie privée et communications électroniques[42], l'un des instruments du cadre relatif aux communications électroniques décrit plus haut, est traitée ici conjointement avec la directive générale relative à la protection des données[43], c'est notamment parce que la première, qui est un instrument sectoriel, précise et complète la seconde (article 1, paragraphe 2, de la directive vie privée et communications électroniques). Toutes deux ont pour objectif « la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel » (article 1, paragraphe 1, de la directive sur la protection des données et article 1, paragraphe 1, de la directive vie privée et communications électroniques, limité toutefois au secteur des communications électroniques). Dans le même temps, elles constituent aussi des instruments du marché intérieur visant à garantir la libre circulation des données à caractère personnel entre Etats membres.

---

[38] Commission européenne, « La Commission se félicite de l'accord supprimant les frais d'itinérance et garantissant un internet ouvert », communiqué de presse, IP/15/5265, 30 juin 2015, http://europa.eu/rapid/press-release_IP-15-5265_fr.htm.

[39] Charte des droits fondamentaux de l'Union européenne, en lien avec l'article 6, paragraphe 1, du traité sur l'Union européenne (version consolidée, traité de Lisbonne), http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:12012P/TXT.

[40] Commission européenne, *op. cit.*, note de bas de page 28.

[41] *Ibid*.

[42] *Op. cit.*, note de bas de page 23.

[43] *Op. cit.*, note de bas de page 24.

La directive sur la protection des données, qui remonte à 1995, sera prochainement remplacée par un texte modernisé. Un nouveau règlement général sur la protection des données (RGPD) est cette année en cours d'adoption par le législateur européen ; il permettra une harmonisation complète des règles relatives à la protection des données personnelles dans toute l'Union[44]. Cette partie se conclut donc par un aperçu des effets réglementaires du RGPD sur le traitement des données à caractère personnel en lien avec les smart TVs, lequel servira de cadre de référence au chapitre IV.

2.3.1. Champ d'application

La directive sur la protection des données s'applique au traitement des données à caractère personnel par des responsables du traitement établis sur le territoire d'un Etat membre ou, dans le cas contraire, lorsque le responsable du traitement recourt, à des fins de traitement de données à caractère personnel, à des moyens situés sur le territoire dudit Etat membre (article 4, paragraphe 1, points a) et c), de la directive). Si le siège de bon nombre de fabricants de smart TVs se situe en dehors de l'Union, la plupart des constructeurs disposent de filiales locales, ce qui ne pose pas de problème pour le champ d'application territorial de la directive.

Dans le cas de services en ligne établis dans des pays tiers auxquels les utilisateurs peuvent avoir accès grâce à leur smart TV interconnectée, deux méthodes permettent d'établir le champ territorial applicable. Tout d'abord, la CJUE a interprété l'article 4, paragraphe 1, point a), de la directive sur la protection des données et estimé qu'il s'appliquait aux responsables du traitement disposant d'un établissement situé dans un Etat membre dont les activités étaient indissociablement liées aux activités de traitement de données du responsable du traitement[45]. Par ailleurs, le groupe de travail « Article 29 » estime que le placement de *cookies* sur l'équipement terminal d'un utilisateur final revient à faire usage d'un appareil situé sur le territoire de l'Union[46]. Conformément à ces interprétations larges, le champ d'application du droit européen relatif à la protection des données devrait englober la plupart des fournisseurs de services en ligne par l'intermédiaire de smart TVs qui se livrent à un traitement des données à caractère personnel des citoyens de l'Union.

2.3.2. Définitions et principes généraux

La directive sur la protection des données comporte des définitions des notions de « données à caractère personnel » et de « traitement » qui sont déterminantes pour le champ d'application matériel défini dans son article 3, paragraphe 1. Il est également important d'introduire la notion de « responsable du traitement », un acteur tenu de respecter la législation relative à la protection des données adoptée par les Etats membres en application des directives, ainsi que la définition du « consentement ». La directive vie privée et communications électroniques reprend dans son article 2 les définitions issues de la directive sur la protection des données.

---

[44] Les projets en cours de discussion dans les réunions de trilogue entre le Conseil, le Parlement européen et la Commission européenne sont disponibles en anglais sur http://data.consilium.europa.eu/doc/document/ST-10391-2015-INIT/en/pdf.

[45] CJUE, affaire C-131/12, *Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos (AEPD),* 13 mai 2014, *par. 56 et 60,* http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:62012CJ0131.

[46] Groupe de travail « Article 29 », document de travail, « Application internationale du droit de l'UE en matière de protection des données au traitement des données à caractère personnel sur internet par des sites web établis en dehors de l'UE », adopté le 30 mai 2002, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2002/wp56_fr.pdf.

2.3.2.1. Données à caractère personnel

Selon l'article 2, paragraphe a), de la directive sur la protection des données, on entend par « données à caractère personnel » « toute information concernant une personne physique identifiée ou identifiable (personne concernée) ». Le groupe de travail « Article 29 », qui réunit les autorités compétentes des Etats membres et de l'Union en matière de protection des données, a publié des lignes directrices sous forme d'un avis concernant l'interprétation précise de chaque élément entrant dans la définition des « données à caractère personnel[47] ». Dans le cas de la télévision intelligente, on peut considérer que les catégories suivantes de données à caractère personnel sont concernées : informations présentes dans le compte de l'utilisateur (le cas échéant), numéro d'identification de l'appareil ou autre identifiant unique (y compris les *cookies*), adresses IP statiques ou dynamiques, habitudes de visionnage et de navigation (suivi des changements de chaînes de télévision, par exemple), profil d'utilisateur personnalisé, données de localisation et commande gestuelle[48] (lorsque cette option est activée). La reconnaissance vocale et faciale, qui peut être mise en œuvre par les fabricants de smart TVs et utilisée sur leurs plateformes numériques, suppose le traitement de données biométriques qui s'apparentent elles aussi à des données à caractère personnel[49].

Dès lors que ces données peuvent être rattachées à une personne physique identifiée ou identifiable, elles constituent des données à caractère personnel au sens de la définition de la directive sur la protection des données. Les utilisateurs sont alors reconnaissables au moyen d'identifiants uniques et l'utilisation de pseudonymes ne détruit pas ce lien avec la personne concernée. C'est la raison pour laquelle les numéros d'identification des appareils et autres identifiants uniques relèvent aussi de la définition des données à caractère personnel donnée par le droit de l'Union en matière de protection des données. A l'inverse, les données anonymisées et anonymes ne constituent plus des données à caractère personnel et leur traitement n'est en conséquence pas couvert par le cadre européen relatif à la protection des données, sauf quand ces données sont à nouveau appliquées à un individu. Il demeure que l'anonymisation des données à caractère personnel doit être conforme aux meilleures pratiques afin que tout risque résiduel d'identification soit écarté[50].

2.3.2.2. Traitement

On entend par « traitement de données à caractère personnel » « toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction » (article 2, point b), de la directive sur la protection des données). Il s'agit donc d'une notion relativement large, de sorte que

---

[47] Groupe de travail « Article 29 », avis 4/2007 sur le concept de données à caractère personnel, adopté le 20 juin 2007, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_fr.pdf.

[48] Liste établie au vu de la jurisprudence évoquée au chapitre III.

[49] Groupe de travail « Article 29 », document de travail sur la biométrie, adopté le 1er août 2003, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2003/wp80_fr.pdf; avis 3/2012 sur l'évolution des technologies biométriques, adopté le 27 avril 2012, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_fr.pdf.

[50] Ce point est souvent négligé, voir groupe de travail « Article 29 », avis 05/2014 sur les techniques d'anonymisation, adopté le 10 avril 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_fr.pdf.

toute opération de traitement réalisée par un responsable du traitement en interne est susceptible de correspondre à cette définition. Du point de vue des atteintes au droit au respect de la vie privée et à la protection des données, et donc de la définition du traitement, il importe peu que les informations communiquées relatives aux vies privées concernées présentent ou non un caractère sensible, ou que le traitement des données à caractère personnel ait importuné les intéressés d'une façon ou d'une autre, ou produit des effets dommageables[51].

2.3.2.3. Responsable du traitement

Ce terme désigne « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel » (article 2, point d), de la directive sur la protection des données). Dans l'écosystème de la télévision intelligente, il existe potentiellement plusieurs responsables du traitement des données à caractère personnel des utilisateurs, tels que les fabricants d'appareils, les fournisseurs de plateformes numériques et de plateformes d'applications, les fournisseurs de services de médias audiovisuels, ainsi que les fournisseurs de contenus et de services en ligne. Dans certaines configurations, leur collaboration peut les amener à être responsables conjoints du traitement, mais dans d'autres cas, ils exercent seuls cette responsabilité. D'autres fournisseurs de services peuvent être concernés pour le volet technique de certains services, tels que des fournisseurs de stockage sur le *cloud* ou de services de reconnaissance vocale qui effectuent des missions et « [traitent] des données à caractère personnel pour le compte du responsable du traitement » (article 2, point e), de la directive sur la protection des données). Ces acteurs sont appelés « sous-traitants » dans la terminologie de la législation sur la protection des données, tant qu'ils conservent leur fonction subordonnée et ne déterminent pas par eux-mêmes de nouvelles finalités ou de nouveaux moyens du traitement des données à caractère personnel.

2.3.2.4. Consentement

Le consentement de la personne concernée est une notion centrale pour légitimer le traitement des données à caractère personnel effectué par le responsable du traitement. Il est défini comme suit : « toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement » (article 2, point h), de la directive sur la protection des données). Le traitement de données à caractère personnel peut reposer sur le consentement indubitable de la personne concernée (article 7, point a)) ; dans certains cas, il est nécessaire de recueillir un consentement explicite, par exemple pour le traitement de catégories particulières de données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ou encore l'appartenance syndicale, ainsi que pour le traitement des données relatives à la santé et à la vie sexuelle (article 8, paragraphe 1, et article 8, paragraphe 2, point a)). Lorsqu'il est procédé à une collecte de données auprès d'une personne, il est nécessaire, pour que le consentement soit valable, que le responsable du traitement ait fourni à celle-ci des informations claires et complètes, conformément à la liste figurant dans l'article 10 de la directive.

---

[51] Voir CJUE, affaires jointes C-465/00, C-138/01 et C-139/01, *Österreichischer Rundfunk* et autres, 20 mai 2003, par. 75, http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:62000CJ0465 ; affaires jointes C-293/12 et C-594/12, *Digital Rights Ireland et Seitlinger c. Minister for Communications, Marine and Natural Resources*, 8 avril 2014, par. 33, http://eur-lex.europa.eu/legal-content/FR/TXT/?qid=1446899221432&uri=CELEX:62012CJ0293.

2.3.3. Directive vie privée et communications électroniques

La directive vie privée et communications électroniques étant un instrument sectoriel, son champ d'application aborde le traitement des données à caractère personnel sous l'angle des communications électroniques. Les obligations découlant de la directive concernent les fournisseurs de réseaux de communications électroniques accessibles au public et aux services de communications électroniques publics, tels qu'ils sont définis dans la directive « cadre » évoquée plus haut. Ceci exclut les fournisseurs de contenus, l'exercice d'une responsabilité éditoriale sur les contenus, ainsi que les services de la société de l'information. Sur le fond, la directive réglemente les droits des utilisateurs et des abonnés de services de communications électroniques (y compris les personnes morales), protège la confidentialité des communications et établit des règles pour l'utilisation des données relatives au trafic et des données de localisation. Elle ne concerne en conséquence qu'une petite portion des parties prenantes à la fois, alors que le poids économique du traitement des données à caractère personnel par les services numériques ne cesse de s'accroître.

La plupart des dispositions de la directive vie privée et communications électroniques ne sont pas adressées aux fabricants de smart TVs ou aux fournisseurs de plateformes numériques, pas plus qu'aux chaînes de télévision ou aux fournisseurs de services de la société de l'information distribués par l'intermédiaire de smart TVs. En revanche, en tant qu'opérateurs de réseaux de communications électroniques accessibles au public, les fournisseurs de services HbbTV[52] (et donc du canal retour) et les câblo-opérateurs sont soumis à la directive. Les fournisseurs de services de communications électroniques publics accessibles sur smart TVs (tels que la téléphonie sur IP ou les conversations vidéo) sont également concernés. Il n'existe que deux exceptions à cette règle, lesquelles s'appliquent de façon horizontale à tous les acteurs économiques : d'une part, l'exigence posée par l'article 5, paragraphe 3, de la directive vie privée et communications électroniques, relative au stockage des informations et à l'accès aux informations déjà stockées dans l'équipement terminal d'un abonné ou d'un utilisateur (également appelée « règle des *cookies* ») ; de l'autre, les dispositions relatives aux communications commerciales non sollicitées (article 13 de la directive vie privée et communications électroniques). A en croire le considérant 8 de la directive « cadre », les smart TVs relèvent du cadre réglementaire relatif aux communications électroniques en leur qualité d'équipements utilisateurs pour la télévision numérique et, en conséquence, l'article 5, paragraphe 3, de la directive vie privée et communications électroniques s'applique :

> *« Les Etats membres garantissent que le stockage d'informations, ou l'obtention de l'accès à des informations déjà stockées, dans l'équipement terminal d'un abonné ou d'un utilisateur n'est permis qu'à condition que l'abonné ou l'utilisateur ait donné son accord, après avoir reçu, dans le respect de la directive 95/46/CE, une information claire et complète, entre autres sur les finalités du traitement. Cette disposition ne fait pas obstacle à un stockage ou à un accès techniques visant exclusivement à effectuer la transmission d'une communication par la voie d'un réseau de communications électroniques, ou strictement nécessaires au fournisseur pour la fourniture d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur. »*

Pour placer des *cookies* ou des pixels espions (« *beacons* ») dans les smart TVs, ou pour accéder à des informations stockées dans l'appareil, les différents acteurs doivent systématiquement obtenir le consentement de l'utilisateur et respecter l'obligation d'information fixée par la directive sur la

[52] L'initiative HbbTV (*Hybrid broadcast broadband TV*) vise à harmoniser à l'échelle mondiale les modalités de distribution de contenus de divertissement en radiodiffusion et par réseau à large bande, par l'intermédiaire des téléviseurs connectés, récepteurs numériques et appareils multi-écrans. Pour de plus amples informations, voir www.hbbtv.org/.

protection des données. En d'autres termes, les fabricants d'appareils et les autres fournisseurs de services sont tenus d'afficher un avertissement relatif au respect de la vie privée avant de stocker des *cookies* ou d'accéder aux informations conservées dans la smart TV[53]. En tout état de cause, l'utilisateur doit se voir offrir la possibilité de refuser le traitement de ses données par le responsable du traitement. Toutefois, la conservation d'informations ou l'accès à des informations déjà stockées dans l'équipement terminal sont licites dans la mesure où ils sont strictement nécessaires pour fournir un service de la société de l'information explicitement demandé par l'abonné ou l'utilisateur.

2.3.4. Directive sur la protection des données

En substance, les responsables du traitement sont tenus de traiter les données à caractère personnel loyalement et licitement, dans le respect des principes énoncés dans l'article 6 de la directive sur la protection des données. Ces principes, pour l'essentiel, évitent la question de la portée, de l'ampleur, de la finalité et de la durée du traitement des données à caractère personnel, pour donner effet aux principes de traitement licite, de spécification et de limitation des finalités du traitement, mais aussi de minimisation des données. Le traitement doit en outre reposer sur l'un des fondements juridiques énumérés à l'article 7 de la directive sur la protection des données qui légitiment le traitement des données : parmi eux figure le consentement indubitable de la personne concernée au traitement de ses données, ainsi que nous l'avons défini plus haut. S'agissant de leurs données, les personnes concernées ont le droit d'obtenir des informations concernant les activités de traitement et les données à caractère personnel détenues par le responsable du traitement, ce qui comprend le droit d'exiger la rectification, l'effacement ou le verrouillage de ces données (article 12, points a) et b) de la directive). En outre, l'article 14 de la directive reconnaît à la personne concernée le droit de s'opposer au traitement dans certaines circonstances, y compris en s'opposant à un traitement de données par ailleurs légitime, par exemple dans le cadre de communications commerciales, conformément à l'article 13, paragraphe 2, de la directive vie privée et communications électroniques.

Les dispositions relatives à la protection des données doivent être appliquées au cas par cas à chaque opération de traitement et en fonction de la finalité poursuivie. L'interprétation des principes et du fondement légitime peut ainsi différer d'une situation à l'autre. Pour les besoins du raisonnement, on différencie couramment les finalités primaires et secondaires, la finalité primaire du traitement de données coïncidant avec un élément du service souhaité par l'utilisateur. La finalité secondaire, elle, relève plutôt de l'intérêt du responsable du traitement et consiste par exemple en l'emploi de publicités contextuelles ou comportementales. En voici quelques exemples :

- L'achat d'une smart TV est avant tout un contrat de vente qui n'a que peu de rapport, voire aucun, avec le traitement de données à caractère personnel, hormis sous l'angle des mises à jour techniques et éventuellement logicielles. Tout traitement supplémentaire de données à caractère personnel nécessiterait un motif légitime autre que l'affirmation selon laquelle le traitement est nécessaire à l'exécution du contrat.
- Les services personnalisés proposés via le guide électronique de programmes nécessitent l'observation et le traitement des habitudes et comportements des téléspectateurs individuels. Dans le cas d'un utilisateur qui s'abonne spécifiquement à des services personnalisés, dès lors qu'il est informé de l'ampleur et de la finalité du traitement de ses

[53] Concernant par exemple les allégations selon lesquelles une smart TV lirait les fichiers présents sur les clés USB et les communiquerait au fabricant, voir Arthur C., « Information commissioner investigates LG snooping smart TV data collection », *The Guardian*, 21 novembre 2013, www.theguardian.com/technology/2013/nov/21/information-commissioner-investigates-lg-snooping-smart-tv-data-collection.

données à caractère personnel, ce traitement peut être nécessaire à l'exécution du contrat, c'est-à-dire à la finalité primaire (article 7, point b), de la directive sur la protection des données). Toutefois, la notion de « ce qui est nécessaire à l'exécution du contrat » doit être interprétée de façon restrictive, de manière à couvrir exclusivement les situations dans lesquelles le traitement est véritablement *nécessaire* à l'exécution d'un contrat[54].

- Lorsque le responsable du traitement souhaite introduire une finalité supplémentaire (secondaire) pour l'utilisation de ces mêmes données à caractère personnel – par exemple la création de profils individualisés en vue de proposer de la publicité contextuelle ou comportementale – il est nécessaire qu'il recueille le consentement indubitable de la personne concernée.
- Un autre fournisseur – par exemple une chaîne de télévision accessible au public (service de médias audiovisuels linéaire) – ne pourrait pas établir valablement que l'observation des habitudes et comportements du téléspectateur individuel est indispensable à l'exécution du contrat, dans la mesure où il s'agit d'une chaîne programmée de façon linéaire et diffusée au plus grand nombre. Pour que le traitement des données à caractère personnel soit légitime, le responsable du traitement doit recueillir le consentement indubitable de la personne concernée.

Surtout, les réglages par défaut d'une smart TV ou d'un service en ligne diffusé par son intermédiaire devraient refléter un état de fait antérieur à tout consentement donné par l'utilisateur au traitement de ses données à caractère personnel. Chaque utilisateur doit être en mesure de contrôler la collecte et l'utilisation de ses données dans les préférences et réglages du téléviseur.

Il est évident au vu de ce qui précède que l'application et le respect des textes de l'Union relatifs à la protection des données ne constituent pas un exercice statique mais fluctuent fortement selon les circonstances propres à chaque activité de traitement. Il serait donc vain de tenter d'énumérer toutes les finalités possibles pour lesquelles les données à caractère personnel pourraient être traitées par chaque acteur de l'écosystème de la télévision intelligente et de développer l'application concrète des règles relatives à la protection des données.

2.3.4.1. Confidentialité et sécurité des traitements

La directive sur la protection des données contient également des exigences relatives à la confidentialité et à la sécurité des traitements. Son article 16 oblige toute personne employée par le responsable du traitement ou ayant pour mission de traiter des données à caractère personnel et qui a accès à de telles données à suivre à la lettre les instructions du responsable du traitement. Selon l'article 17 de la directive, « le responsable du traitement doit mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite ». Dans le contexte des flux de données à caractère personnel liés aux smart TVs, cette disposition serait interprétée comme requérant des flux cryptés et des mesures permettant le respect des trois piliers de la sécurité de l'information : confidentialité, intégrité et disponibilité des données.

[54] Groupe de travail « Article 29 », avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE, adopté le 9 avril 2014 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_fr.pdf.

2.3.4.2. Flux de données internationaux

Enfin, en vertu de la législation de l'Union relative à la protection des données, le transfert de données à caractère personnel de l'Union vers un pays tiers n'est autorisé que si ledit pays garantit un degré adapté de protection des données ou si l'une des dérogations prévues par l'article 26 de la directive sur la protection des données s'applique. Si, par exemple, une smart TV collecte des données à caractère personnel auprès de résidents de l'Union et les transfère à un fabricant de matériel dont le siège est situé dans un pays tiers, cette transaction entraîne un transfert international de données[55]. Ce type de transfert n'est autorisé que s'il est avéré que le pays tiers offre un degré de protection adéquat des données à caractère personnel[56]. En l'absence d'appréciation de ce degré d'adéquation par la Commission européenne, ces transferts internationaux peuvent être effectués sur la base de règles d'entreprise contraignantes, de clauses contractuelles standard ou, en dernier recours, du consentement indubitable de la personne concernée (article 26, paragraphes 1 et 4, de la directive sur la protection des données).

2.3.5. Nouveau règlement sur la protection des données

Ainsi que nous l'avons évoqué, les propositions à l'étude de règlement général sur la protection des données (RGPD) élargiraient le champ d'application territorial de la réglementation aux situations dans lesquelles le responsable du traitement n'est pas établi dans l'Union européenne, lorsque les activités de traitement sont liées a) à l'offre de biens ou de services, qu'un paiement soit exigé ou non, aux personnes concernées, ou b) à leur observation. Une fois adopté, ce règlement permettrait de clarifier certains points et d'instaurer des innovations réglementaires, notamment concernant les smart TVs. Si le principe de séparation est confirmé par le législateur de l'Union, par exemple, on considérera que la personne concernée ne donne son consentement « librement » que si elle a aussi la possibilité de ne pas le faire. Les fournisseurs de services devront également mettre en place un environnement dans lequel les utilisateurs peuvent refuser le traitement de leurs données à caractère personnel pour des finalités secondaires.

Le projet de RGPD introduit également de nouvelles règles s'agissant du profilage et des principes de protection des données dès la conception et par défaut.

Les principes de la protection des données dès la conception et par défaut entraînent un devoir, pour les responsables du traitement et leurs sous-traitants, de mettre en œuvre des mesures techniques et organisationnelles adaptées et proportionnées tenant compte de l'état de la technique, des connaissances techniques actuelles, des pratiques d'excellence internationales et des risques que présentent les procédures de traitement des données.

[55] *Ibid.*

[56] Voir CJUE, affaire C-362/14, *Maximillian Schrems c. Data Protection Commissioner*, 6 octobre 2015, http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:62014CJ0362.

2.4. Directive sur le commerce électronique et législation de l'Union relative à la protection du consommateur

La directive sur le commerce électronique[57] complète la réglementation des services en ligne qui, d'une part, ne sont pas des services publics de communications électroniques consistant entièrement ou principalement en la transmission de signaux électroniques et, d'autre part, ne sont pas des services de médias audiovisuels linéaires tels que la radiodiffusion télévisée[58]. Conformément à la terminologie de la directive sur le commerce électronique, ces services sont des services de la société de l'information, définis en référence à une autre directive[59]. On entend ainsi par « services de la société de l'information » « tout service presté normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services » (article 2, point a), de la directive sur le commerce électronique, en lien avec l'article 1, paragraphe 1, de la directive 98/34/CE telle que modifiée par la directive 98/48/CE[60]). L'écosystème de la télévision intelligente peut englober de nombreux services de la société de l'information, tels que la vidéo à la demande, les guides électroniques de programmes, mais aussi les applications et les boutiques qui les commercialisent, entre autres.

La directive sur le commerce électronique ne met pas en place une réglementation exhaustive de ces services ; elle entend principalement établir un marché intérieur pour eux et rendre possible la conclusion de contrats par voie électronique. Toutefois, elle impose aux fournisseurs de services de la société de l'information une série d'exigences relativement élaborées s'agissant des informations à fournir en lien avec les communications commerciales (articles 5 et 6).

La directive prévoit en outre une série de dérogations en matière de responsabilité pour certains prestataires intermédiaires qui assurent des services de transit (« simple transport »), de « *caching* » et d'hébergement (articles 12 à 14). Dans l'écosystème de la télévision intelligente, toutes ces fonctionnalités sont indéniablement présentes ; toutefois, afin de pouvoir bénéficier d'une dérogation en matière de responsabilité, un service donné proposé par un fournisseur doit être précisément conforme à la définition correspondante dans la directive. Par exemple, une plateforme numérique assurant le *caching* ou l'hébergement de services de médias audiovisuels et de contenus en ligne de parties tierces ne peut bénéficier de cette dérogation que si « [cette] activité revêt un caractère purement technique, automatique et passif, qui implique que le prestataire de services de la société de l'information n'a pas la connaissance ni le contrôle des informations transmises ou stockées » (considérant 42).

Il importe de relever que la directive sur le commerce électronique ne saurait anticiper l'évolution de la réglementation de l'Union en matière de protection des données. Son considérant 14 précise donc que « [la] mise en œuvre et l'application de la présente directive devraient être conformes aux principes relatifs à la protection des données à caractère personnel ».

La directive relative aux droits des consommateurs[61] fait partie de l'acquis de l'Union dans ce domaine. Elle concourt au rapprochement des dispositions nationales relatives à la vente de biens et de services (y compris les contrats à distance et hors établissement) entre professionnels et

---

[57] *Op. cit.*, note de bas de page 25.

[58] Considérant 18, *Op. cit.*, note de bas de page 25.

[59] Directive 98/34/CE du Parlement européen et du Conseil du 22 juin 1998 prévoyant une procédure d'information dans le domaine des normes et réglementations techniques et des règles relatives aux services de la société de l'information, telle que modifiée par la directive 98/48/CE, et codifiée par la Directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015, http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32015L1535&from=EN.

[60] *Ibid.*

[61] Directive 2011/83/UE du Parlement européen et du Conseil du 25 octobre 2011 relative aux droits des consommateurs, http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32011L0083.

consommateurs. Elle réglemente en particulier les contrats de fourniture de contenu numérique[62]. Le considérant 19 de la directive définit le contenu numérique comme suit : « les données qui sont produites et fournies sous une forme numérique, comme les programmes informatiques, les applications, les jeux, la musique, les vidéos ou les textes, que l'accès à ces données ait lieu au moyen du téléchargement ou du streaming, depuis un support matériel ou par tout autre moyen. » A côté des règles générales relatives à la protection du consommateur, telles que le droit de rétractation, on notera qu'au moment de la conclusion du contrat, en sus des exigences générales d'information qui lui incombent, le fournisseur est tenu d'informer le consommateur des fonctionnalités et de l'interopérabilité du contenu numérique concerné[63]. Par fonctionnalités, on doit cependant aussi entendre les usages du contenu numérique servant par exemple à observer le comportement des consommateurs. Ceci vaut pour la vente de contenus numériques commercialisés par contrat à distance, hors établissement et par des contrats autres (articles 5 et 6 de la directive). En complément des exigences d'information découlant de la législation européenne relative à la protection des données, la directive sur le droit des consommateurs est un exemple de plus de texte législatif exigeant que le consommateur ait préalablement connaissance du suivi opéré de son comportement.

2.5. Cadre relatif aux droits de l'homme

Comme nous l'avons déjà mentionné, le cadre européen relatif aux droits de l'homme met l'accent sur le droit au respect de la vie privée et à la protection des données. Les dispositions les plus importantes à cet égard sont l'article 8 de la Convention européenne des droits de l'homme (« Droit au respect de la vie privée et familiale »), ainsi que les articles 7 (« Respect de la vie privée et familiale ») et 8 (« Protection des données à caractère personnel ») de la Charte des droits fondamentaux de l'Union européenne. Les principes établis dans ces dispositions, approfondis ultérieurement par la jurisprudence, fournissent de précieuses orientations quant à la nature et à la portée des droits de l'homme et des droits fondamentaux au respect de la vie privée et à la protection des données. Le champ d'application de l'article 8 de la CEDH s'étend à la protection des données à caractère personnel, bien que cela ne soit pas explicitement indiqué. La séparation opérée par la charte entre droit au respect de la vie privée et droit à la protection des données à caractère personnel tient compte de l'évolution du droit relatif à la protection des données, domaine à part, soumis à une législation sectorielle. Il est toutefois utile de rappeler le lien sous-jacent entre vie privée et données à caractère personnel en ce qui concerne les smart TVs. La fonction de reconnaissance vocale de ces derniers, associée à leur capacité de capter des conversations menées dans l'intimité du foyer, soulève des inquiétudes compréhensibles pour le droit à la vie privée et familiale.

Malgré l'importance de ces dispositions relatives aux droits de l'homme, leur applicabilité aux fournisseurs de services par l'intermédiaire des smart TVs est une question complexe. La CEDH, à l'instar des traités internationaux, ne crée des obligations que pour les autorités étatiques, et non pour les parties privées, en règle générale. Ainsi que l'ont expliqué certains commentateurs de renom, la CEDH ne donne pas lieu à un effet horizontal ou *Drittwirkung*, une interprétation selon laquelle « un individu peut s'appuyer sur une charte des droits nationale pour déposer plainte contre une personne physique qui a porté atteinte à ses droits garantis par cet instrument[64] ». Pour autant,

[62] *Ibid.*, considérant 19.

[63] *Ibid.*

[64] Harris D. J. et al., *Law of the European Convention on Human Rights* (3e édition), Oxford University Press, Oxford, 2014, p. 23.

cela ne signifie pas que la CEDH ne peut avoir une incidence directe sur le comportement des parties privées, par exemple par l'intermédiaire des obligations positives qu'elle impose aux Etats[65]. En outre, la législation nationale peut également s'emparer de ces questions.

L'article 1 de la CEDH impose aux parties contractantes de « [reconnaître] à toute personne relevant de leur juridiction les droits et libertés » définis dans la convention. L'obligation de « reconnaître » ces droits est explicite et sous-entend nécessairement qu'ils ne sont pas « théoriques ou illusoires, mais concrets et effectifs[66] ». Afin de garantir ces droits, il ne suffit pas toujours que l'Etat se contente de ne pas s'immiscer dans les droits des individus : des actions positives et constructives sont nécessaires en complément. Dans certains cas, la CEDH prévoit explicitement des obligations positives, par exemple dans les articles 6 (« Droit à un procès équitable ») et 13 (« Droit à un recours effectif »). Tous deux présupposent indéniablement une action constructive de la part des Etats, si les droits garantis ne sont pas réalisés dans les faits. Au-delà de ces obligations positives explicites contenues dans la CEDH, la Cour a également identifié au fil des ans différentes obligations positives sous-entendues par le texte[67].

Dans son arrêt *Airey c. Irlande*, la Cour a affirmé que « si l'article 8 (art. 8) a essentiellement pour objet de prémunir l'individu contre des ingérences arbitraires des pouvoirs publics, il ne se contente pas d'astreindre l'Etat à s'abstenir de pareilles ingérences : à cet engagement plutôt négatif peuvent s'ajouter des obligations positives inhérentes à un respect effectif de la vie privée ou familiale[68] ». Dans l'affaire *X et Y c. Pays-Bas*, elle a complété cette affirmation en admettant que ces obligations positives « peuvent impliquer l'adoption de mesures visant au respect de la vie privée jusque dans les relations des individus entre eux[69] ». Il s'agit là d'une extension importante du principe tel qu'il était formulé dans la jurisprudence antérieure ; elle confirme que certains droits sont, dans une certaine mesure, applicables horizontalement. La Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel établit un cadre législatif destiné à être mis en place par les Etats signataires[70]. La Cour se réfère souvent à ce texte dans les affaires touchant au traitement automatisé des données à caractère personnel[71].

De la même façon, il est important de garder à l'esprit l'applicabilité particulière de la Charte des droits fondamentaux de l'Union européenne. Ses dispositions « s'adressent aux institutions, organes et organismes de l'Union dans le respect du principe de subsidiarité, ainsi qu'aux Etats membres uniquement lorsqu'ils mettent en œuvre le droit de l'Union » (article 51, paragraphe 1). « En conséquence, ils respectent les droits, observent les principes et en promeuvent l'application, conformément à leurs compétences respectives et dans le respect des limites des compétences de l'Union telles qu'elles lui sont conférées dans les traités. » (*ibid.*) Les dispositions de la charte « contiennent des principes [qui] peuvent être mis en œuvre par des actes législatifs et exécutifs pris

---

[65] *Ibid*.

[66] Arrêt de la Cour européenne des droits de l'homme, affaire *Airey c. Irlande*, requête n° 6289/73, 9 octobre 1979, série A n° 32, par. 24, http://hudoc.echr.coe.int/fre?i=001-61978.

[67] Pour une analyse détaillée, voir, généralement, Mowbray A., *The Development of Positive Obligations under the European Convention on Human Rights by the European Court of Human Rights*, Hart Publishing Ltd., Oxford, 2004.

[68] Arrêt *Airey c. Irlande*, *op.cit.*, note de bas de page 66, par. 32.

[69] Arrêt de la Cour européenne des droits de l'homme, affaire *X et Y c. Pays-Bas*, requête n° 8978/80, 26 mars 1985, série 1 n° 91, par. 23, http://hudoc.echr.coe.int/fre?i=001-62162.

[70] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STCE n° 108) et Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données (STCE n° 181), www.coe.int/fr/web/conventions/full-list/-/conventions/rms/0900001680078b39.

[71] Voir, par exemple, arrêt de la Cour européenne des droits de l'homme, affaire *Amann c. Suisse*, requête n° 27798/95, 16 février 2000, par. 65, http://hudoc.echr.coe.int/fre?i=001-62971.

par les institutions, organes et organismes de l'Union, et par des actes des Etats membres lorsqu'ils mettent en œuvre le droit de l'Union, dans l'exercice de leurs compétences respectives » (article 52, paragraphe 5). Toutefois, « [leur] invocation devant le juge n'est admise que pour l'interprétation et le contrôle de la légalité de tels actes » (*ibid.*).

3. Etudes de cas par pays

La position conjointe ainsi que le test technique allemands portent sur chacune des quatre fonctions identifiées des smart TVs – reconnaissance vocale, contrôle gestuel, reconnaissance faciale et création de compte. Les affaires néerlandaises TP Vision et Ziggo, pour leur part, abordent en particulier l'aspect de la création de compte, tandis que la plainte américaine de l'EPIC auprès de la FTC porte sur les capacités de reconnaissance vocale.

Ces études de cas nationales illustrent tout d'abord, avec l'exemple de la position conjointe adoptée en Allemagne, la manière dont des lignes directrices pourraient être élaborées dans ce domaine et dont les autorités (de protection des données) pourraient réglementer les nombreuses implications juridiques des smart TVs. Deuxièmement, l'affaire néerlandaise illustre spécifiquement les questions juridiques relatives à la protection des données et au respect de la vie privée qui sont en jeu. L'exemple américain vient ensuite mettre à jour les implications plus larges de la réglementation des smart TVs, touchant entre autres aux domaines des télécommunications, de la protection des enfants et de la protection des consommateurs.

3.1. Allemagne

Dans le contexte de tests réalisés, au printemps 2014[72], par un institut de consommateurs allemands qui réalise des essais de produits (*Stiftung Warentest*), les questions du respect de la vie privée et de la protection des données à caractère personnel des membres du public et des utilisateurs des fonctions interactives des smart TVs ont fait les gros titres. Cet institut indépendant a critiqué en particulier la fonctionnalité HbbTV, dont il a été établi qu'elle communiquait les données de consommation des médias par les utilisateurs aux chaînes de télévision et à plusieurs tierces parties, y compris Google. L'institut a également estimé que le fait qu'un téléviseur connecté utilise la reconnaissance faciale pour proposer des recommandations personnalisées de programmes de télévision et de contenus en ligne constituait une intrusion dans la sphère privée des utilisateurs, principalement dans la mesure où la politique de confidentialité du fabricant lui réservait le droit de transmettre les données personnelles à des parties tierces. D'autres fonctionnalités, telles que la caméra et le microphone intégrés, n'avaient pas été considérés comme problématiques à l'époque. Néanmoins, l'institut recommandait d'éviter l'usage de la reconnaissance vocale dans la mesure où il s'agit d'une caractéristique biométrique individuelle.

A la suite de ces conclusions, les autorités allemandes de protection des données se sont intéressées de près à la question de la conformité des téléviseurs connectés avec les lois locales sur la protection des données. De manière coordonnée, les autorités compétentes des Etats fédérés

[72] Stiftung Warentest, « Ausgespäht : Datenschutz beim Fernsehen », test 5(2014) https://www.test.de/filestore/4697612_t201405040.pdf?path=/protected/46/21/2b850438-9820-4bc1-bcfb-12f9cb905c2f-protectedfile.pdf.

(*Länder*) ont adopté une position conjointe[73] et lancé un test technique pour analyser les flux de données personnelles transmises à partir des téléviseurs connectés[74]. En septembre 2015, ce processus a abouti à l'adoption, par les autorités allemandes de protection des données compétentes, de lignes directrices précisant les obligations des services de smart TV en matière de protection des données[75].

3.1.1. La position conjointe

La position conjointe, intitulée « La télévision intelligente, seulement avec une protection des données intelligente » (« *Smartes Fernsehen nur mit smartem Datenschutz*[76] »), est le fruit d'un accord entre les autorités de protection des données chargées de mettre en œuvre les lois relatives à la protection des données dans le secteur privé (le « *Düsseldorfer Kreis* ») et les organismes chargés de la protection des données des opérateurs de médias de service public, et fait, avant tout, l'objet du soutien de la conférence des autorités des médias (*Konferenz der Direktoren der Landesanstalten für Medien*).

La position conjointe s'ouvre en expliquant qu'il est difficile, pour le public et les utilisateurs de téléviseurs connectés, de faire la différence entre consommation de télévision linéaire, accès à des contenus via internet ou combinaison des deux éléments, dans la mesure où la réception des signaux audiovisuels et l'interactivité avec internet via un canal retour sont désormais intégrés. Les utilisateurs ne sont généralement pas en mesure d'identifier quel service ils sont en train d'utiliser. Au contraire de la télévision traditionnelle, la connexion internet s'accompagne d'un canal retour, transmettant des informations émanant de l'utilisateur vers le fournisseur de télévision, le fabricant de l'équipement ou d'autres parties tierces. Grâce à ce canal, il est possible de suivre et d'analyser le comportement des utilisateurs individuels.

La position conjointe se poursuit en établissant un lien entre le droit de rechercher des informations et le suivi et l'utilisation des données relatives au comportement de l'utilisateur. Elle affirme que le droit à rechercher des informations, qui constitue une partie intégrante du droit à la liberté d'expression dans la loi fondamentale allemande (*Grundgesetz*) et qui est un fondement d'une constitution libre et démocratique, serait limité par le suivi et l'utilisation des données qui s'y rattachent.

La position conjointe énumère ensuite les obligations qui s'imposent en vertu de la loi allemande applicable en matière de protection des données, c'est-à-dire la loi sur les télémédias (*Telemediengesetz*)[77]. En droit allemand, les services de télémédias sont définis de manière similaire aux services de la société de l'information en vertu de la directive e-commerce, et incluent ainsi les services de communication et d'information électroniques qui ne constituent ni de la radiodiffusion ni une simple transmission de signaux électroniques (paragraphe 1 (1) de la loi sur les télémédias). La position conjointe fournit des indications quant à la manière dont les dispositions juridiques s'appliquent à la smart TV.

---

[73] En allemand : Gemeinsame Position der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) und der Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten, « Smartes Fernsehen nur mit smartem Datenschutz », mai 2014,

http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/Beschluss_SmartTV.html.

[74] Bayrisches Landesamt für Datenschutzaufsicht, « Datenschutz und Smart TV », communiqué de presse du 27 février 2015, https://www.datenschutz-mv.de/presse/2015/pm-SmartTV.pdf.

[75] *Op cit*., note de bas de page 7.

[76] *Op cit*., note de bas de page 73.

[77] Loi sur les télémédias du 26 février 2007, modifiée pour la dernière fois par l'article 4 de la loi du 17 juillet 2015 http://www.gesetze-im-Internet.de/tmg/BJNR017910007.html.

1. L'utilisation anonyme de services de télévision doit être possible également dans le contexte de la smart TV. Le profilage de la consommation individuelle de télévision n'est pas permis sauf si le consentement éclairé et explicite de l'utilisateur a été obtenu.
2. Lorsque des services en ligne ou HbbTV sont utilisés via des téléviseurs connectés, ils sont soumis à la réglementation sur les télémédias et doivent se conformer aux obligations en matière de protection des données de la loi allemande sur les télémédias. Les fabricants d'équipement, les chaînes de télévision et autres fournisseurs de services en ligne considérés comme des télémédias sont tenus d'obtenir le consentement des utilisateurs ou – au minimum – de se conformer aux dispositions juridiques suivantes :
    a. Les données personnelles des utilisateurs peuvent être traitées si cela est nécessaire à la fourniture où la facturation du service.
    b. Au plus tard lorsque qu'ils commencent à utiliser le service, les utilisateurs doivent être informés de manière manifeste et complète du recueil et de l'utilisation de leurs données personnelles.
    c. Les fournisseurs de services de télémédias ne sont autorisés à créer et analyser des profils individuels d'usage et de consommation que s'ils recourent à des pseudonymes et si l'utilisateur concerné ne s'y est pas opposé. Un tel refus doit impérativement être suivi d'effets, et, notamment, les informations stockées dans l'équipement de l'utilisateur (par exemple, les cookies) doivent être effacées. Les fournisseurs doivent informer les utilisateurs de leur droit de refus. Les adresses IP et les numéros d'identification de l'appareil ne constituent pas des pseudonymes au sens de la loi allemande sur les télémédias.
    d. Les organismes internes compétents doivent s'assurer que les profils d'utilisation ne sont pas réassociés avec l'utilisateur individuel lié au pseudonyme.
3. Le principe du « respect de la vie privée par défaut » doit être appliqué : les fabricants et les fournisseurs doivent s'assurer que les paramètres par défaut des téléviseurs connectés et des services en ligne disponibles respectent le principe de l'usage anonyme du téléviseur. L'accès aux services en ligne et les échanges de données en ligne qui en découlent entre le fabricant de l'équipement, le fournisseur du service et d'autres fournisseurs ne peuvent prendre place que si l'utilisateur en a fait la requête après avoir reçu des informations complètes, par exemple avec l'activation du HbbTV via le « bouton rouge ». Les utilisateurs doivent être en mesure de contrôler l'information stockée dans l'équipement. En particulier, il doit leur être possible de gérer les cookies.
4. Les téléviseurs connectés, les services HbbTV des chaînes de télévision et les autres services en ligne doivent appliquer des mesures de sécurité techniques qui protègent les équipements et les données de tout accès non autorisé par des parties tierces.

3.1.2. Le test technique

Au début de 2015, un test technique coordonné à l'échelle nationale et dirigé par l'Autorité bavaroise de protection des données (*Bayerisches Landesamt für Datenschutzaufsicht*), a été mené sur les téléviseurs connectés de 13 fabricants, représentant environ 90 pour cent du marché allemand[78]. L'objectif du test technique n'était pas de vérifier la conformité d'appareils ou de fabricants donnés avec les lois pertinentes allemandes en matière de protection des données. Le test visait d'abord à améliorer la compréhension, du point de vue technique, des flux de données

[78] *Op cit*., note de bas de page 74.

circulant à partir des téléviseurs connectés et à mieux comprendre les rôles des différents acteurs impliqués. Dans le détail, le test technique s'est concentré sur les devoirs d'information des fabricants d'équipements et sur l'analyse des flux de données en lien avec les services HbbTV, les app stores et les services de recommandations personnalisées. Le cryptage des flux de données issus des téléviseurs connectés est essentiel du point de vue de la sécurité, mais il a également limité la portée du test technique, dans la mesure où il n'a pas été possible de vérifier la nature exacte des informations transmises.

Le paragraphe suivant propose un bref résumé des résultats du test, sur la base d'un exposé présenté lors de la conférence de presse du 27 février 2015[79] :

- Sur les 13 téléviseurs connectés testés, six fournissaient des informations en lien avec le respect de la vie privée et la protection des données avant que l'équipement ne soit connecté à internet.
- Sept chaînes de télévision sur 10 suivent, grâce à la fonction HbbTV (« bouton rouge »), les changements de chaîne de l'utilisateur.
- Huit chaînes de télévision sur 10 informent les utilisateurs de la fonction HbbTV du traitement de données à caractère personnel et sollicitent leur consentement.
- Six téléviseurs connectés sur 13 cryptent les données lors de l'usage des app stores qui sont préinstallés sur l'équipement ; sur les sept téléviseurs connectés qui communiquent avec les app stores de manière non cryptée, cinq transmettent le nom de l'application que l'utilisateur a lancée.
- Lorsque les utilisateurs reçoivent des recommandations personnalisées via le guide électronique des programmes (EPG)[80], sept téléviseurs connectés sur 13 envoient des communications de manière cryptée au serveur de l'EPG. Pour les six autres téléviseurs connectés, aucun flux de données n'a été détecté.
- Lorsque les utilisateurs connectent un dispositif de stockage externe au téléviseur connecté, ici une clé USB, quatre équipements sur 13 envoyaient des communications cryptées[81].
- Sur les 12 téléviseurs connectés équipés d'une fonction enregistrement, un communiquait l'enregistrement et les cinq autres envoyaient des communications cryptées.
- Lors de la consommation de télévision linéaire, l'ensemble des 10 chaînes testées recevaient des données via le canal retour, ainsi que quatre des 13 fabricants d'équipements.

A la suite du test technique, les autorités de protection des données compétentes des Etats fédérés (*Länder*) ont préparé un document de référence sur la smart TV, qui vise à appuyer les actions d'application et de mise en œuvre. En parallèle, les autorités de protection des données compétentes vont se rapprocher des fabricants afin d'obtenir des clarifications supplémentaires et de déterminer ce qui devra être fait pour que leurs téléviseurs connectés soient conformes aux dispositions relatives à la protection des données.

[79] Bayerisches Landesamt für Datenschutzaufsicht, « Technische Pruefung SmartTV », conférence de presse du 27 février 2015. https://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/SmartTV_Technische%20Pr%C3%BCfung%20Druck.pdf.

[80] A la condition que le consentement ait été donné pour tout traitement de données personnelles.

[81] En lien avec des allégations antérieures selon lesquelles les téléviseurs connectés accèdent aux documents présents sur les clés USB et les communiquent au fabricant, voir Arthur C., « Information commissioner investigates LG snooping smart TV data collection », *op.cit*.

3.1.3. Document de référence sur les obligations en matière de protection des données des services de smart TV

Lors de sa session des 15-16 septembre 2015, les autorités allemandes de protection des données pour le secteur privé, regroupées au sein du *Düsseldorfer Kreis*, ont adopté un nouveau document de référence sur les obligations des services de smart TV en matière de protection des données[82]. Le document s'adresse aux fournisseurs de services et produits de smart TV, en particulier les fabricants d'équipement, les portails d'applications et les fournisseurs d'applications, les services de recommandations personnalisées et les fournisseurs de HbbTV. Le document fournit un aperçu approfondi de la manière dont les autorités de protection des données compétentes évaluent les activités de ces fournisseurs vis-à-vis de la loi allemande sur la protection des données (*Bundesdatenschutzgestz*).

Le document explique de façon précise les services des téléviseurs connectés impliquant des flux de données personnelles, et fournit également des définitions et des explications des concepts clés en droit allemand de la protection des données. Le document de référence a le mérite de reposer sur une approche globale des questions de protection des données au sein de l'écosystème de la smart TV, qui aborde les divers acteurs et services impliqués, et qui tient également compte de l'intégration verticale de la chaîne de valeur[83]. Ainsi, sur la base d'une approche modulaire, les obligations allemandes en matière de protection des données sont déclinées pour toute une gamme de services fournis par les téléviseurs connectées impliquant des flux de données personnelles.

L'évaluation se fonde sur le droit allemand en matière de protection des données, qui déroge à certains aspects importants du droit de l'UE en la matière, tel que le décrit le chapitre 2. En principe, les lignes directrices prévoient les circonstances dans lesquelles le cadre juridique allemand donne une base juridique pour le traitement des données personnelles ou celles dans lesquelles un utilisateur individuel doit donner son consentement explicite au traitement des données personnelles. La loi allemande sur les télémédias (*Telemediengesetz*) établit une distinction entre usage des informations de l'abonné (*Bestandsdaten*) et usage des données d'utilisation (*Nutzungsdaten*) des utilisateurs individuels, qui doivent respecter des obligations juridiques différentes. En particulier, en vertu de la loi sur les télémédias, les utilisateurs ont le droit d'utiliser les services identifiés comme télémédias de manière anonyme, dans la mesure où cela est techniquement possible. Ainsi, les utilisateurs doivent disposer d'un choix en la matière. Cette obligation n'existe pas, par exemple, en droit européen de la protection des données.

Une autre particularité de la loi sur les télémédias est que les fournisseurs de service sont autorisés à créer des profils d'utilisateurs rattachés à des pseudonymes dans un objectif publicitaire ou pour mener des recherches sur le marché, et en vue de fournir les services demandés, sauf en cas d'objection de l'utilisateur (c'est-à-dire qu'il existe un droit de refus[84]). La pseudonymisation s'accompagne cependant de l'obligation de dissocier le profil d'usage lié au pseudonyme de l'utilisateur individuel du service. Cette obligation n'est pas respectée si les profils d'utilisateur sont associés aux numéros d'identification des équipements ou aux adresses IP.

Une importance toute particulière est portée aux obligations d'information, qui constituent un prérequis en vertu de la loi allemande sur la protection des données, et qui doivent être mises en œuvre avant tout traitement des données personnelles[85]. Les utilisateurs devraient également pouvoir, à tout moment, accéder aux informations concernant l'utilisation de leurs données

[82] Düsseldorfer Kreis, *ibid*. note de bas de page 73.

[83] *Ibid*.

[84] *Ibid.*

[85] *Ibid.*

personnelles. Le document précise que le fait d'intégrer l'information dans les conditions générales du service ne suffit pas, en droit allemand de la protection des données, à satisfaire l'obligation de transparence. En outre, le droit allemand de la protection des données reprend les principes de protection des données qui sont également connus en droit de l'UE.

Une autre série importante de dispositions porte sur la capacité des utilisateurs à gérer les paramètres et les préférences sur leur appareil, y compris les cookies, et sur l'obligation d'un paramétrage par défaut conçu de façon à respecter la vie privée dans le cadre des services en ligne HbbTV et des microphones et caméras intégrés[86].

Enfin, il faut souligner que les lignes directrices précisent les mesures techniques et organisationnelles nécessaires pour protéger la sécurité des données personnelles. En particulier, les fabricants d'équipements doivent procéder à des mises à jour régulières au niveau de la sécurité, et tous les flux de données personnelles entre le téléviseur connecté et les fournisseurs de services doivent être cryptés pendant leur transmission, entre autres.

La position conjointe décrite ci-dessus constitue un document d'orientation, tandis que les lignes directrices adoptées par la suite précisent de manière plus détaillée la façon dont les autorités allemandes en matière de protection des données interpréteront et appliqueront la loi, dans le cadre du traitement de données personnelles par les divers acteurs intervenant dans l'écosystème de la smart TV. Les lignes directrices appliquent de manière stricte les dispositions allemandes pertinentes en matière de données personnelles issues de la loi sur les télémédias ainsi que de la loi fédérale sur la protection des données. Elles ne vont pas au-delà des dispositions prévues au niveau législatif, qui sont déjà, de toute façon, plutôt strictes. Le résultat le plus significatif des lignes directrices est la mise en place d'une approche modulaire pour l'évaluation, du point de vue juridique, des activités spécifiques impliquant un traitement de données personnelles, quel que soit le rôle du fournisseur dans l'écosystème de la smart TV.

3.2. Les Pays-Bas

L'Autorité néerlandaise de protection des données (« *College bescherming persoonsgegevens* » – CBP) a enquêté sur deux sociétés commerciales impliquées dans le traitement de données personnelles en lien avec des services de télévision numérique interactive et des services en ligne proposés via des téléviseurs connectés. Le CBP est chargé de vérifier la conformité des offres avec la loi néerlandaise sur la protection des données[87] (« *Wet bescherming persoonsgegevens* » – WBP), qui met en œuvre la directive de l'UE sur la protection des données, examinée en détail au chapitre 2 sur les cadres réglementaires européens[88]. En cas de violation de la loi néerlandaise, le CBP peut utiliser ses pouvoirs d'exécution et imposer par exemple des amendes conditionnelles[89].

[86] *Ibid.*

[87] Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens), http://wetten.overheid.nl/BWBR0011468/geldigheidsdatum_26-10-2015.

[88] Chapitre 2, dans « Réglementation sur le respect de la vie privée et les communications électroniques, ainsi que sur la protection des données ».

[89] https://www.cbpweb.nl/en/node/1930.

Selon le CBP, le traitement des données personnelles portant sur les habitudes de consommation – dans le contexte du thème plus général du « suivi et traçage » – mérite une attention particulière[90]. La première enquête concernait TP Vision : une société proposant des services de smart TV via des équipements Philips. La deuxième enquête portait sur le câblo-opérateur Ziggo, qui propose des médias audiovisuels à ses abonnés. En raison de l'analyse détaillée de la loi néerlandaise sur la protection des données, ces exemples, au-delà des implications juridiques qu'ils soulèvent au niveau néerlandais, identifient également des questions pertinentes concernant le cadre européen de la protection des données applicable à la smart TV.

Nous examinerons d'abord séparément les circonstances factuelles et juridiques des deux affaires, puis nous analyserons, dans une conclusion aux exemples néerlandais, les implications futures pour la réglementation de la smart TV.

3.2.1. Exemple 1 – *CBP c. TP Vision*

Le 2 juillet 2013, l'Autorité néerlandaise de protection des données a publié ses conclusions relatives à la société néerlandaise TP Vision, qui fabrique les Smart TV Philips[91]. Le CBP a enquêté sur le traitement des données personnelles des utilisateurs de Smart TV Philips aux Pays-Bas. Le CBP affirme que TP Vision enfreignait la loi néerlandaise sur la protection des données (WBP) en raison de l'absence d'informations claires, accessibles et complètes sur le traitement des données personnelles, d'un consentement éclairé pour le placement de cookies de traçage et de contrats avec les parties tierces. Les données traitées par TP Vision sont issues des fonctions « création de compte » et des fonctionnalités interactives des téléviseurs connectés, tels que décrites ci-dessus[92].

Nous examinerons en premier lieu le contexte factuel de l'enquête du CBP sur les téléviseurs connectés TP Vision. Le cadre juridique sous-tendant le rapport du CBP sur les téléviseurs connectés TP Vision sera ensuite analysé.

3.2.1.1. Contexte factuel

C'est en raison de l'augmentation de la vente de téléviseurs équipés de fonctionnalités interactives et de services à la demande qui recueillent des informations relatives aux utilisateurs que le CBP a été amené à enquêter sur les téléviseurs connectés, et en particulier sur TP Vision. TP Vision développe et produit les Smart TV de Philips, dont 1.2 millions d'exemplaires auraient été vendus aux Pays-Bas depuis 2009. TP Vision recueille et stocke des données relatives au comportement en ligne des téléspectateurs, à l'usage des applications et à l'historique des sites internet consultés – par exemple en recourant à des cookies (de traçage). En outre, les Smart TV de TP Vision recueillent des données relatives aux habitudes des utilisateurs, telles que : leurs programmes et applications préférés, les programmes qu'ils enregistrent, les vidéos qu'ils louent, et les programmes qu'ils ont

[90] Autorité néerlandaise de protection des données, Enquête sur le traitement des données personnelles via le recours aux services interactifs de télévision numérique de Ziggo, Rapport du 28 avril 2015, https://cbpweb.nl/sites/default/files/atoms/files/onderzoek_ziggo.pdf. Autorité néerlandaise de protection des données, Rapport annuel 2014, https://cbpweb.nl/sites/default/files/atoms/files/annual_report_2014.pdf.

[91] Autorité néerlandaise de protection des données, Enquête sur le traitement des données personnelles sur les Smart TV Philips par TV Vision Netherlands B.V., Rapport du 2 juillet 2013, https://www.cbpweb.nl/sites/default/files/downloads/pb/pb_20130822-persoonsgegevens-smart-tv.pdf.

[92] Chapitre 1.

visionnés à la demande. Sur la base de ces données, TP Vision leur propose des recommandations personnalisées et envisage de présenter des publicités personnalisées à l'avenir.

3.2.1.2. Cadre juridique

Le CBP a d'abord procédé à un examen approfondi des pratiques de TP Vision et des autres circonstances de l'affaire, puis il a examiné ces activités et pratiques à la lumière de la WBP. Parmi les diverses obligations prévues par la WBP, l'enquête du CBP s'est concentrée sur les exigences principales de la notion de donnée à caractère personnel, la base juridique pour le traitement des données personnelles, les obligations d'information et les contrats avec les parties tierces.

3.2.1.2.1. Données personnelles

Les données personnelles sont définies par la WBP comme « toute information relative à une personne physique identifiée ou identifiable[93] ». Dans la mesure où la définition présente les mêmes caractéristiques que celle retenue par la directive de l'UE sur la protection des données et précisée par le Groupe de travail Article 29, l'examen détaillé des « données à caractère personnel » fourni au chapitre 2 suffit à donner une idée précise de ce rapport du CBP. Selon le CBP, les données recueillies ici constituent des données personnelles, dans la mesure où les informations collectées par TP Vision – entre autres, les adresses IP, les programmes de télévision visionnés, les applications utilisées et les sites web consultés – donnent un aperçu détaillé des habitudes télévisuelles, du comportement et des préférences des utilisateurs[94]. En outre, le CBP qualifie ces données personnelles de sensibles par nature, puisqu'elles révèlent beaucoup sur les individus concernés[95]. Elles peuvent par exemple indiquer une origine sociale particulière, un profil financier et/ou une situation familiale. Par conséquent, ce type de données pourrait être utilisé pour influencer le comportement (en ligne) des utilisateurs, à des fins de marketing direct ou pour le profilage des utilisateurs de Smart TV. Cette approche mérite d'être soulignée car elle fait des données personnelles à caractère sensible une catégorie distincte des autres catégories de données personnelles protégées par ailleurs, qui révèlent des informations liées à la santé, aux croyances religieuses, aux opinions politiques etc.

TP Vision détermine les objectifs et les moyens du traitement des données personnelles. TP Vision doit donc être considéré comme le « responsable du traitement » des données personnelles issues des téléviseurs connectés[96]. Encore une fois, la définition du « responsable du traitement » correspond à la définition du cadre européen décrit ci-dessus.

3.2.1.2.2. Information

Selon la WBP, les responsables du traitement des données doivent fournir des informations spécifiques aux personnes concernées : l'identité du responsable du traitement, les objectifs du

[93] Article 1(a) de la WBP ; article 1(a) de la directive sur la protection des données. Pour plus d'informations, voir : Groupe de travail Article 29, WP 136, Avis 4/2007 sur le concept de données à caractère personnel, 20 juin 2007.

[94] Pour une liste exhaustive des données collectées, voir : Autorité néerlandaise de protection des données, Enquête sur le traitement des données personnelles sur les Smart TV Philips par TV Vision Netherlands B.V., Rapport du 2 juillet 2013.

[95] *Ibid*.

[96] Article 1(d) de la WBP ; article 2(d) de la directive sur la protection des données. Pour plus d'informations sur les notions de « responsable du traitement » et de « sous-traitant », voir l'Avis 01/2010 sur les notions de responsable du traitement et de sous-traitant adopté le 16 février 2010 (WP 169), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_fr.pdf.

traitement des données, les destinataires des données, et l'existence de leur droit d'accès et de leur droit de refus[97]. Ces informations doivent être fournies d'une façon claire et intelligible, dans l'objectif de donner à l'utilisateur davantage de contrôle sur la dissémination de ses données personnelles.

Le CBP a estimé que TP Vision ne se conformait pas à ces obligations d'information. Les consommateurs n'étaient informés ni sur le site internet de Philips, ni par la politique de confidentialité de TP Vision, ni par un bandeau d'information sur les cookies ou encore par les conditions d'utilisation. De manière plus précise, les utilisateurs ne recevaient pas d'information sur l'existence et les responsabilités de TP Vision, sur le placement des cookies, sur le type de données recueillies, ou sur la durée de conservation de ces données.

Au cours de l'enquête, TV Vision a ajusté sa déclaration de confidentialité, sa politique en matière de cookie ainsi que ses conditions d'utilisation pour se mettre en conformité. Néanmoins, selon le CBP, l'information est toujours insuffisamment claire, contradictoire et inaccessible au public. En particulier, l'information n'est pas présentée en néerlandais, dans un format court et facile à lire, et en outre, l'information n'est pas fournie en avance mais après que la Smart TV a été connectée à internet.

3.2.1.2.3. Base juridique pour le traitement des données personnelles

Dans son rapport, le CBP affirme que TP Vision accède aux informations des utilisateurs par le biais de cookies. Du fait de ce recours aux cookies, la société doit également se conformer à la loi néerlandaise sur les télécommunications[98].

Lorsqu'un responsable du traitement stocke des données ou accède à des données déjà conservées sur un appareil, l'utilisateur concerné doit consentir à ce stockage ou à cet accès pour que ces actions soient légitimes – à moins qu'elles ne soient « *strictement nécessaires afin de fournir un service explicitement demandé par l'abonné ou l'utilisateur*[99] ». En vertu de la loi néerlandaise sur les télécommunications – et de la directive européenne sur la vie privée susmentionnée – le consentement de l'utilisateur doit être basé sur une information claire et complète fournie par le responsable du traitement et portant, entre autres, sur les objectifs du traitement.

En outre, les cookies placés par TP Vision traitent des données personnelles. Ainsi, le responsable du traitement doit disposer d'une base juridique pour que ce traitement de données personnelles soit légitime en vertu de la WBP[100].

Pour le CBP, TP Vision doit obtenir un « consentement indubitable » avant de pouvoir recueillir des données personnelles via des cookies. Ce consentement doit être basé sur l'expression d'une intention libre, spécifique et informée. Initialement, TP Vision ne demandait aucune permission, bien que cette politique ait été ultérieurement modifiée. De plus, le consentement n'est pas donné librement, puisqu'il est requis pour l'installation du téléviseur connecté. Ainsi l'utilisateur est tenu d'accepter les conditions d'usage. Cela était également vrai lorsque TP Vision utilisait des « pop-up » ouvrant une possibilité de refus (« opt-out ») en vue d'obtenir le consentement, dans la mesure où seule la possibilité d'accepter (« opt-in ») est considérée comme une libre expression de l'intention.

Deuxièmement, tel que nous l'avons évoqué plus haut, TP Vision ne fournit pas une information claire et accessible sur l'usage des cookies et sur les spécificités du traitement qui en est

[97] Articles 33 et 34 de la WBP ; articles 10 et 11 de la directive sur la protection des données.

[98] Loi néerlandaise sur les télécommunications du 19 octobre 1998 (« *Telecommunicatiewet* » – Tw), http://www.wetboek-online.nl/wet/Telecommunicatiewet.html.

[99] Article 11.7a(3)(b) de la Tw.

[100] Article 8 de la WBP ; article 7 de la directive sur la protection des données.

fait. Cette absence de transparence implique que le consentement au traitement des données n'est pas valide, puisqu'il n'est ni « spécifique » ni « éclairé ».

3.2.1.2.4. Contrat de sous-traitance

TP Vision recourt aux services de plusieurs sociétés pour le traitement des données personnelles. Dans la mesure où ces sociétés peuvent être considérées comme des « sous-traitants » au sens de la loi néerlandaise sur la protection des données, TP Vision est tenu de conclure avec elles un contrat de sous-traitance ou un autre acte juridique qui couvre les responsabilités des deux parties, afin de garantir le traitement équitable des données personnelles[101].

Le CBP a affirmé que TP Vision n'était pas en conformité avec cette disposition, puisqu'aucun contrat de sous-traitance n'avait été signé avec Google pour l'utilisation des services Google Analytics. Google, cependant, a refusé de signer le contrat, et le problème a donc été réglé en mettant un terme à toute coopération avec Google. TP Vision avait déjà signé des contrats avec les autres sous-traitants pour lesquels, selon le CBP, seuls des ajustements mineurs étaient nécessaires pour se conformer avec la WBP.

A la suite de l'enquête du CBP, TP Vision a amendé sa déclaration de confidentialité, sa politique en matière de cookies et ses conditions d'utilisation afin de mettre ses pratiques en conformité avec la WBP. Les informations relatives à la collecte de cookies de suivi du comportement du téléspectateur sont présentées de manière plus claire au moment de l'installation du téléviseur connecté et, de plus, des informations claires et complètes sur le traitement des données dans un objectif publicitaire sont disponibles. Comme indiqué ci-dessus, le CBP estime que TP Vision est toujours en infraction avec la loi néerlandaise relative à la protection des données. Néanmoins, le CBP a annoncé que, dans la mesure où il a été mis un terme partiel à l'infraction, il n'aurait pas recours à des actions d'exécution formelles[102]. Le CBP continuera cependant à surveiller la conformité de TP Vision avec la WBP.

3.2.2. Exemple 2 - *CBP c. Ziggo*

Le 28 avril 2015, l'Autorité néerlandaise de protection des données a publié son rapport d'enquête sur le câblo-opérateur Ziggo. Le rapport explique comment Ziggo a violé la loi néerlandaise sur la protection des données en suivant le comportement de visionnage des utilisateurs de services numériques interactifs. Ces données personnelles, tout comme dans l'affaire TP Vision, se réfèrent aux fonctions « création de compte » et aux fonctionnalités interactives des téléviseurs connectés, telles que décrites dans le détail au chapitre 1. Selon le CBP, Ziggo a enfreint la WBP en ne fournissant pas aux utilisateurs des informations suffisantes sur le traitement des données personnelles. De plus, l'enquête a conclu que Ziggo n'avait pas obtenu le consentement indubitable requis pour le traitement des données personnelles.

Nous analyserons en premier lieu le contexte factuel du rapport du CBP, puis nous exposerons le cadre juridique sur lequel s'est fondé l'examen par le CBP des services interactifs de Ziggo.

[101] Article 14 de la WBP ; article 17(4) de la directive sur la protection des données.

[102] Voir https://www.cbpweb.nl/nl/nieuws/tp-vision-past-privacybeleid-aan-na-onderzoek-cbp.

3.2.2.1. Contexte factuel

Ziggo B.V. est un câblo-opérateur de télévision néerlandais qui propose des services interactifs de télévision numérique. Bien que Ziggo ait récemment fusionné avec le fournisseur UPC Nederland, l'examen du CBP a pris place avant cette fusion et ne tient donc compte que des actes et activités de Ziggo. La raison qui a poussé le CBP à enquêter sur Ziggo est que Ziggo constituait, avec 2.3 millions d'utilisateurs, le plus grand fournisseur de services de télévision numérique des Pays-Bas. Aujourd'hui, les services de Ziggo comptent 4.2 millions de consommateurs.

Dans son rapport, le CBP examine trois formes différentes de suivi du comportement des téléspectateurs pour déterminer comment Ziggo utilise ces données à des fins de profilage et de marketing. Le CBP se concentre sur la consommation « traditionnelle » (c'est-à-dire linéaire) de télévision, la consommation (de vidéos) à la demande, et le visionnage en paiement à l'acte. S'agissant de la première catégorie, le visionnage de télévision en linéaire, Ziggo était en mesure de définir le comportement de visionnage d'individus spécifiques et, en conséquence, de déterminer des taux d'audience à plus grande échelle. Le rapport du CBP explique que Ziggo traitait ces données personnelles grâce à un décodeur de télévision interactif activé.

Dans le cas des services à la demande, Ziggo, également grâce à des décodeurs interactifs, était à même de connaître l'historique de visionnage des utilisateurs. Sur la base du profilage du comportement des utilisateurs de vidéos à la demande, Ziggo proposait des recommandations de visionnage personnalisées en fonction des utilisateurs et était également en mesure de fournir des recommandations de visionnage en général.

Troisièmement, le CBP a examiné séparément le suivi du « paiement à l'acte » ou « paiement à l'événement ». Le paiement à l'acte est un service interactif grâce auquel les utilisateurs peuvent acheter certains programmes ou films en ligne, principalement dans les domaines sportif et érotique. Ziggo utilisait ces informations sur les téléspectateurs de manière ponctuelle dans un objectif de marketing direct.

3.2.2.2. Cadre juridique

Le CBP ouvre son rapport avec une description approfondie des aspects procéduraux et des circonstances factuelles du traitement par Ziggo des données personnelles. Ensuite, le CBP examine les actions et les pratiques de Ziggo à la lumière de la WBP. Comme dans l'affaire TP Vision, l'enquête du CBP se concentre – parmi les diverses obligations de la WBP – sur la notion de donnée personnelle, sur l'obligation d'information et sur la base juridique pour le traitement des données. Nous allons examiner ces obligations en suivant la distinction établie par le CBP entre consommation linéaire, à la demande et par paiement à l'acte. Le CBP identifie des infractions à la loi relative à la protection des données dans chacun de ces domaines.

3.2.2.2.1. Données personnelles

Selon le CBP, Ziggo recueille des données personnelles en suivant le comportant des téléspectateurs. En analysant et/ou en affinant ces données, Ziggo est en mesure de classifier les utilisateurs selon des profils spécifiques et de les traiter différemment ou de manière plus ciblée.

Le CBP a notamment relevé le caractère sensible des données personnelles concernées par les activités de traitement de données de Ziggo. Comme le CBP l'a déterminé dans l'affaire TP Vision, ces données personnelles devraient être considérées comme sensibles, dans la mesure où le suivi de la consommation de la télévision numérique – notamment l'historique de la consommation en paiement à l'acte de contenus érotiques – révèle de manière intrusive les habitudes et les préférences des utilisateurs. Ces données peuvent indiquer une origine sociale, un profil financier

et/ou une situation familiale. Par conséquent, ce type de données pourrait être utilisé pour influencer le comportement (en ligne) des utilisateurs, ou dans des objectifs de marketing ou de profilage des utilisateurs de Ziggo[103].

3.2.2.2.2. Information

Comme indiqué précédemment, la WBP exige que les responsables du traitement des données doivent communiquer des informations spécifiques aux personnes concernées, telles que l'identité du responsable, les objectifs du traitement et l'existence de leur droit d'accès en lien avec le traitement de leurs données personnelles[104]. Ces informations doivent être fournies de manière claire et intelligible, dans le but de donner aux utilisateurs davantage de contrôle sur la dissémination de leurs données personnelles.

Dans la première catégorie examinée, à savoir les services de télévision linéaire, Ziggo était à même de déterminer le comportement de visionnage d'individus particuliers, sans que la personne concernée ne dispose d'informations suffisantes. Selon le CBP, Ziggo n'a pas suffisamment précisé le type de données collectées et traitées et les objectifs spécifiques du traitement.

Ziggo a mis un terme à cette infraction en ajustant les décodeurs de manière à ce qu'il ne soit plus possible d'associer les informations relatives au comportement de visionnage à des individus spécifiques. Avec ces méthodes d'anonymisation, les données traitées ne peuvent plus être considérées comme des données personnelles. Ainsi, à la suite de ces modifications, la loi néerlandaise en matière de protection des données n'est plus applicable, ce qui selon le CBP règle également, entre autres, les infractions précédentes à la loi.

S'agissant de la télévision à la demande, Ziggo n'a pas fourni d'informations suffisantes sur de multiples aspects. D'abord, la politique de confidentialité de Ziggo affirmait que toutes les informations étaient traitées de manière anonyme, ce que le CBP a jugé mensonger. De plus, les utilisateurs n'étaient pas informés du type de données comportementales traitées. Troisièmement, Ziggo ne respectait pas son devoir d'information, dans la mesure où il ne précisait pas les objectifs du traitement. L'objectif « d'adapter les services aux [besoins des] clients » n'est pas suffisamment précis. De plus, les utilisateurs ne savent pas que leur comportement de visionnage est utilisé afin d'établir leur profil. Enfin, d'une façon générale, la politique de confidentialité de Ziggo n'était pas accessible à la plupart des consommateurs, dans la mesure où il était difficile de trouver la déclaration de confidentialité sur le site internet de Ziggo.

Dans la dernière catégorie, la consommation à l'acte, Ziggo ne respectait pas non plus son devoir d'information. Le suivi de la consommation numérique (à caractère sensible) était mis en œuvre sans que Ziggo informe ses utilisateurs d'aucun aspect du traitement. De manière générale, les usagers ne savaient pas que Ziggo établissait le profil de leur comportement de visionnage dans des objectifs de marketing.

3.2.2.2.3. Base juridique pour le traitement des données personnelles

La WBP exige que le responsable du traitement dispose d'une base juridique pour que le traitement des données personnelles soit légitime[105]. Le CBP affirme que Ziggo enfreint cette disposition en raison du suivi de la consommation linéaire, à la demande, et en paiement à l'acte, en l'absence de consentement valide. Le CBP a précisé que Ziggo ne pouvait s'appuyer sur aucune autre base

[103] *Ibid*.

[104] Articles 33 et 34 de la WBP ; articles 10 et 11 de la directive sur la protection des données.

[105] Article 8 de la WBP ; article 7 de la directive sur la protection des données.

juridique que l'obtention d'un « consentement indubitable » pour ce traitement, car il concernant des données sensibles.

En ce qui concerne la première catégorie, la télévision linéaire, le CBP a estimé que Ziggo n'avait pas obtenu le consentement indubitable requis avant de procéder au traitement des données personnelles des utilisateurs. A l'époque, Ziggo ne donnait pas aux utilisateurs la possibilité d'exprimer leur consentement à quelque moment que ce soit au cours du processus de collecte des données. Comme indiqué ci-dessus, en rendant anonymes les données traitées, la violation de la disposition de la WBP a été réglée, dans la mesure où il n'était plus possible d'associer les informations relatives au comportement de visionnage à des individus en particulier.

Selon le CBP, l'utilisation des données personnelles tirées de la consommation à la demande constituait une violation de la WBP. Ziggo n'avait pas obtenu un consentement éclairé valide ; les utilisateurs n'avaient pas de possibilité effective de refuser de donner leur accord à ce traitement des données.

Initialement, Ziggo ne demandait aucun consentement. Par la suite, Ziggo a introduit un bouton dit de « refus ». D'autres tentatives de formuler la requête de manière plus spécifique avaient été effectuées, mais sans remédier au fait que les informations fournies quant au type de données personnelles collectées étaient insuffisantes. Selon le CBP, Ziggo n'informe pas les utilisateurs quant aux catégories précises de données personnelles utilisées afin de personnaliser les contenus. En outre, comme indiqué ci-dessus, Ziggo n'informe pas les utilisateurs de la création de profils. De plus, cette possibilité n'était proposée qu'aux nouveaux utilisateurs, et pas aux utilisateurs antérieurs de Ziggo. Dans la mesure où le consentement constitue, selon le CBP, une stricte obligation, il découlait de son absence que les activités de Ziggo étaient illégales. Ziggo a à nouveau adapté ses activités à la demande, et il est désormais demandé aux consommateurs d'accorder (ou non) un consentement valide pour le traitement de leurs données personnelles[106].

Dans la dernière catégorie du visionnage en paiement à l'acte, les informations relatives aux téléspectateurs étaient utilisées de manière ponctuelle pour des activités de marketing direct. Ce qui a été relevé pour la télévision linéaire et à la demande se vérifie également pour cette catégorie. Dans la mesure où, en particulier, les informations sont qualifiées par le CBP de données personnelles sensibles, Ziggo enfreignait la WBP car il avait omis de requérir un consentement valide.

En réponse au rapport du CBP, Ziggo a mis un terme aux infractions à la WBP en procédant à de multiples ajustements de sa politique en matière de confidentialité. Le CBP estime que Ziggo est désormais en conformité avec les obligations prévues par la WBP, car il informe les abonnés de manière adaptée et requiert leur consentement indubitable pour le traitement de leurs données personnelles[107].

3.2.2.3. Implications pour l'avenir

D'une façon générale, le CBP reconnaît que, dans la mesure où les téléviseurs connectés sont relativement récents sur le marché de la télévision, les consommateurs sont peu conscients des risques qui découlent de leur utilisation. Il est donc probable que le CBP continue de s'intéresser à ce phénomène nouveau, afin de protéger les droits des abonnés et des utilisateurs de services interactifs de smart TV. Dans le cadre de ses responsabilités, le CBP met au premier plan la question de la sensibilisation aux impacts sur la vie privée et la protection des données des équipements

[106] CBP Persbericht, *« Ziggo beëindigt privacy overtredingen digitale tv na onderzoek CBP »*, 9 juin 2015, https://cbpweb.nl/nl/nieuws/ziggo-beeindigt-privacyovertredingen-digitale-tv-na-onderzoek-cbp.

[107] *Ibid*.

interactifs, tels que les téléviseurs interactifs, qui mettent facilement en lien de multiples aspects de la vie privée des individus[108]. Aux Pays-Bas, il n'existe pas (encore) d'alliance, sur le modèle allemand, entre autorités chargées du respect de la vie privée et organisations de médias publics – ni d'autres formes de coordination transversale du secteur.

3.2.2.3.1. Télévision interactive

Les deux enquêtes illustrent l'approche de l'Autorité néerlandaise de protection des données consistant à mener des actions d'application choisies qui servent d'exemples pour le traitement des données personnelles dans le contexte des services interactifs des téléviseurs connectés. L'enquête portant sur Ziggo souligne des aspects intéressants du suivi et du profilage des utilisateurs de télévision interactive. L'étendue des possibilités des téléviseurs connectés est abordée en tenant compte des distinctions entre visionnage de la télévision en linéaire, à la demande, et par paiement à l'acte. En revanche, dans l'affaire TP Vision, d'autres services liés aux téléviseurs connectés étaient abordés, tels que le suivi du comportement en ligne des téléspectateurs, de l'utilisation des applications, et de l'historique de consultation des sites internet en général[109]. De plus, le CBP confirme que les informations relatives à l'historique de visionnage de l'utilisateur, qu'il s'agisse d'un visionnage à la demande ou en paiement à l'acte, peuvent être considérées comme des données personnelles sensibles. Une telle approche pourrait également être retenue pour d'autres équipements interactifs qui suivent les comportements individuels.

3.2.2.3.2. Le rôle de l'information et de la transparence

Il ressort clairement des deux exemples néerlandais que c'est l'absence d'une information suffisante de la personne concernée qui constitue l'aspect primordial de l'infraction. Ce devoir d'information est une exigence spécifique en droit néerlandais (et européen) de la protection des données. Il influence également la validité du consentement, puisque ce dernier doit se fonder sur une expression « éclairée » de l'intention. Il est possible d'en conclure que cet aspect relatif à l'information en matière de protection des données joue un rôle fondamental.

Les rapports néerlandais démontrent tout deux l'importance de la transparence dans le domaine des équipements interconnectés des consommateurs. L'accroissement de la transparence quant aux caractéristiques du traitement des données personnelles et des contrats de sous-traitance devrait améliorer la prise de décision et la possibilité pour les utilisateurs d'avoir un contrôle effectif sur leurs données personnelles.

A l'instar de la réglementation des médias qui vise à donner davantage d'autonomie aux individus (éducation aux médias), la réglementation en matière de protection des données cherche à atteindre ce même objectif d'autonomisation et de transparence. D'autres dispositions de la WBP, telles que le droit d'accès des personnes concernées, devrait donner plus de contrôle aux individus par rapport aux responsables du traitement des données personnelles.

Ainsi, le CBP s'est attaché à résoudre les infractions constatées dans ces deux affaires principalement afin de donner davantage de contrôle aux individus. Les affaires néerlandaises n'abordent pas le droit relatif à la protection des consommateurs. Néanmoins, la volonté de rendre

[108] Le Groupe de travail Article 29 a publié un rapport sur l'importance de la transparence dans le domaine des dispositifs interconnectés, voir : Groupe de travail Article 29, avis 8/2014 sur les développements récents de l'internet des objets, WP 223, 16 septembre 2014.

[109] Autorité néerlandaise de protection des données, Enquête sur le traitement des données personnelles sur les Smart TV Philips par TV Vision Netherlands B.V., Rapport du 2 juillet 2013.

les individus plus autonomes peut être considérée comme semblable à l'objectif que poursuit la réglementation en matière de protection des consommateurs, que nous allons examiner plus loin.

De plus, la position conjointe allemande explique que le problème du manque d'information découle principalement du fait que les signaux audiovisuels et l'interactivité avec internet via un canal retour sont désormais intégrés. Le test technique des téléviseurs connectés a révélé que, sur les 13 téléviseurs connectés testés, six fournissaient des informations en lien avec le respect de la vie privée et la protection des données avant que l'équipement ne soit connecté à internet[110].

3.3. Un exemple américain

Le point intéressant de l'étude de cas américaine ci-dessous est que l'EPIC propose différentes pistes, au niveau réglementaire, pour une action de la Federal Trade Commission contre Samsung. Comme l'expose le chapitre 2, (au moins) cinq types de réglementation sont applicables aux téléviseurs connectés. A la différence des affaires néerlandaises, cette étude de cas illustre la possibilité d'agir contre des activités de traitement des données supposément proscrites (enregistrement de la voix) en se fondant sur la protection des consommateurs – et en particulier des enfants – ainsi que sur les lois relatives au respect de la vie privée et aux télécommunications. Bien qu'il ne soit pas certain que la FTC engage des poursuites sur la base de ces instruments, il est intéressant d'examiner les différentes options envisageables pour la réglementation des téléviseurs connectés aux Etats-Unis.

3.3.1. *Electronic Privacy Information Center c. Samsung*

Le 24 février 2015, l'EPIC (*Electronic Privacy Information Center*)[111] a déposé une plainte auprès de la Federal Trade Commission (FTC) des Etats-Unis à propos des téléviseurs connectés Samsung[112]. Dans cette plainte, l'EPIC affirme que les pratiques commerciales de Samsung affectent le droit au respect de la vie privée des consommateurs aux Etats-Unis, dans la mesure où Samsung intercepte et enregistre de façon routinière les communications privées des consommateurs à leur domicile en utilisant les fonctionnalités d'enregistrement de la voix des téléviseurs connectés. L'EPIC demande à la FTC d'intervenir.

Nous analyserons en premier lieu le contexte factuel de la plainte de l'EPIC, puis nous examinerons le cadre juridique appuyant la plainte de l'EPIC à propos de l'intrusion supposée dans la vie privée des téléviseurs connectés Samsung. Dans la dernière partie, nous nous pencherons sur les implications possibles de la requête de l'EPIC auprès de la FTC.

3.3.1.1. Contexte factuel

La plainte de l'EPIC concerne les capacités de reconnaissance vocale des téléviseurs connectés Samsung. La télécommande « Smart Touch » de Samsung dispose d'un microphone intégré pour

[110] Bayrisches Landesamt für Datenschutzaufsicht, « Technische Pruefung SmartTV », conférence de presse du 27 février 2015 https://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/SmartTV_Technische%20Pr%C3%BCfung%20Druck.pdf.

[111] L'EPIC est un centre de recherche d'intérêt public établi à Washington DC.

[112] EPIC, *In the matter of Samsung Electronics Co., Ltd., EPIC Complaint, Request for Investigation, Injunction and Other Relief*, 24 février 2015, https://epic.org/privacy/internet/ftc/Samsung/EPIC-FTC-Samsung.pdf.

l'enregistrement des voix. Comme expliqué ci-dessus[113], les téléviseurs connectés Samsung peuvent aller plus loin que la simple fonctionnalité de reconnaissance vocale examinée par l'EPIC. Le contrôle gestuel, la reconnaissance faciale et les fonctions de création de compte, ne seront pas examinées dans cet exemple.

Le fondement des allégations de l'EPIC, selon lesquelles Samsung intercepte et enregistre de manière régulière les conversations privées au domicile se trouve dans les politiques de confidentialité précédente[114] et actuelle[115] de Samsung. L'EPIC cite trois sections de ces politiques de confidentialité pour appuyer ses allégations de violation de la vie privée des consommateurs.
La première et principale section citée par l'EPIC se trouve dans la partie « reconnaissance vocale » de la politique de confidentialité précédente : « *Veuillez noter que si les mots que vous prononcez incluent des informations à caractère personnel ou d'autres informations sensibles, ces informations seront incluses dans les données collectées et transmises à une tierce partie via votre utilisation de la fonction reconnaissance vocale*[116] ». Selon l'EPIC, dès lors que la fonction reconnaissance vocale de la smart TV est activée, tous ce qu'un utilisateur dit devant un téléviseur connecté Samsung est enregistré et transmis à une tierce partie par internet – que cela ait ou non un rapport avec la fourniture du service. La « tierce partie » mentionnée dans la politique de confidentialité n'était pas identifiée dans la version précédente de la politique[117]. Samsung a par la suite – en raison de commentaires négatifs à son endroit dans les médias – expliqué que la « tierce partie » était la société Nuance Communications, Inc[118], spécialisée dans la conversion de la voix en texte.

L'EPIC cite en outre une section de la politique de confidentialité actuelle de Samsung : « *Veuillez noter que lorsque vous regardez une vidéo ou accédez aux applications ou aux contenus fournis par une tierce partie, ce fournisseur peut collecter ou recevoir des informations à propos de votre téléviseur connecté (par exemple, son adresse IP et les identifiants de l'appareil), la transaction requise (par exemple, votre demande d'achat ou de location de la vidéo), et votre utilisation de l'application ou du service. Samsung n'est pas responsable des pratiques de ces fournisseurs en matière de respect de la vie privée ou de sécurité. Vous devriez faire preuve de prudence et examiner les déclarations de confidentialité des sites web et services de la partie tierce que vous utilisez*[119] ». Sur la base de cette section, l'EPIC affirme que Samsung tente de se dégager de toute responsabilité quant aux pratiques de tierces parties en matière de respect de la vie privée ou de sécurité, y compris celles de Nuance[120].

Troisièmement, l'EPIC mentionne le fait que Samsung a affirmé qu'il cryptait les communications vocales qu'il transmet à Nuance[121]. Cependant, les chercheurs en informatique Ken Munro et David Lodge ont découvert que Samsung ne crypte pas tous les enregistrements vocaux qu'il réalise et transmet à Nuance[122]. Selon l'EPIC, en réponse à ces conclusions, Samsung a

---

[113] Paragraphe 1.2.

[114] Voir http://global.samsungtomorrow.com/samsung-smart-tvs-do-not-monitor-living-room-conversations/.

[115] Voir http://www.samsung.com/uk/info/privacy-SmartTV.html.

[116] *Op. cit.*, note de bas de page 114.

[117] *Ibid.*

[118] *Ibid.*

[119] *Op. cit.*, note de bas de page 112, paragraphe 24; Samsung Global Privacy Policy http://www.samsung.com/us/common/privacy.html.

[120] *Op. cit.*, note de bas de page 112, para. 23.

[121] *Ibid.* paragraphe 25 ; *« Samsung accorde toute son importance au respect de la vie privée des consommateurs et nos produits sont conçus en tenant compte de ce respect. Nous mettons en œuvre les normes, garanties et pratiques du secteur, y compris le cryptage des données, afin de securiser les informations personnelles des consommateurs et pour en empêcher toute collecte ou utilisation non autorisée ».* http://global.samsungtomorrow.com/samsung-smart-tvs-do-not-monitor-living-room-conversations/.

[122] *Ibid.*, paragraphe 27 ; https://www.pentestpartners.com/blog/is-your-samsung-tv-listening-to-you/.

ultérieurement admis que la société ne cryptait pas toutes les conversations qu'elle transmettait, et qu'elle n'avait pas mis en place les logiciels nécessaires au cryptage des transmissions en clair[123].

L'EPIC étaye sa plainte en citant des experts du droit au respect de la vie privée et en s'appuyant sur les expériences des consommateurs. Selon l'EPIC, les experts du domaine mettent en garde sur le fait que la pratique de Samsung d'un enregistrement vocal « permanent » induit les consommateurs en erreur, et ceux qui ont été mis au courant de cette pratique l'ont décrite comme déloyale et trompeuse[124].

3.3.1.2. Cadre juridique

L'EPIC démontre l'illégalité supposée des téléviseurs connectés Samsung – l'interception et l'enregistrement extensifs mentionnés ci-dessus de conversations privées, l'absence (partielle) de cryptage et la tentative de se dégager de toute responsabilité – en s'appuyant sur la loi sur le câble, la loi sur le respect de la vie privée en matière de communications électroniques, la loi sur la protection de la vie privée des enfants en ligne et la loi relative à la FTC. Le point central de la plainte s'articule autour de la loi relative à la FTC et des déclarations de principe de la FTC correspondantes sur le caractère déloyal et le caractère trompeur.

3.3.1.2.1. La loi sur les communications par câble

L'EPIC se réfère en premier lieu à la loi sur les communications par câble (*Cable Communications Policy Act* - CCPA)[125], dont l'objectif est de protéger les informations personnelles des clients des fournisseurs de services par câble.

La disposition 47 U.S.C. 551 §631(b) de la CCPA prohibe la collecte d'informations pouvant mener à l'identification personnelle d'un abonné sans obtention préalable du consentement, écrit ou par voie électronique, de l'abonné concerné. De plus, la disposition 47 U.S.C. 551 § 631(c) interdit de dévoiler des informations permettant l'identification personnelle d'un abonné[126] et exige que les fournisseurs de câble prennent toutes les mesures nécessaires pour empêcher l'accès non autorisé à de telles informations par une personne autre que l'abonné ou le câblo-opérateur – ce qui concernerait la société de conversion de la voix en texte Nuance.

Au vu de ces exigences, l'EPIC affirme que « *Samsung n'obtient pas de consentement écrit ou par voie électronique pour l'enregistrement des conversations privées des personnes dans leur domicile et pour la transmission de ces enregistrements vocaux à Nuance*[127] ». L'EPIC ajoute que « *Samsung ne prend pas les mesures nécessaires pour empêcher un accès non autorisé aux informations relatives à l'abonné* » et par conséquent, que « *Samsung collecte de manière délibérée et excessive les informations fournies par les abonnés au câble*[128] ». L'EPIC ne précise pas de quelle manière cette collecte excessive est réalisée.

---

[123] *Op. cit.*, note de bas de page 112, paragraphes 28 et 29 ; http://www.bbc.com/news/technology-31523497.

[124] *Ibid.* paragraphes 30-57.

[125] *Cable Communications Policy Act* de 1984 (CCPA), 47 U.S.C. §521-573.

[126] Les exceptions à l'interdiction de divulgation prévues par la disposition 47 U.S.C. 551 § 631(2), telles que les requêtes gouvernementales dans le cadre d'une ordonnance d'un tribunal, ou les divulgations nécessaires à la fourniture des services câblés, ne sont pas applicables dans l'affaire en cause.

[127] *Op. cit.*, note de bas de page 112, paragraphe 60.

[128] *Ibid.* paragraphe 61.

3.3.1.2.2. La loi sur le respect de la vie privée en matière de communications électroniques

La deuxième loi citée par l'EPIC est la loi sur le respect de la vie privée en matière de communications électroniques (*Electronic Communications Privacy Act* - ECPA[129]). L'ECPA protège les communications filaires, verbales et électroniques et s'applique aux emails, aux conversations téléphoniques et aux données stockées sur des supports électroniques.

La disposition 18 U.S.C. § 2511(1) de l'ECPA dispose que toute personne[130] qui, « *de manière intentionnelle, intercepte, tente d'intercepter ou incite toute autre personne à intercepter des communications filaires, verbales ou électroniques*[131] » ou qui, « *de manière intentionnelle, divulgue ou tente de divulguer à toute autre personne le contenu de toute communication filaire, verbale ou électronique, en sachant ou en ayant des raisons de penser que les informations ont été obtenues par l'interception d'une communication filaire, verbale ou électronique, en violation avec cette sous-section*[132] », enfreint l'ECPA.

L'EPIC affirme que Samsung enfreint l'ECPA en interceptant et en enregistrant les communications privées des personnes à leur domicile[133], dans la mesure où il intercepte ces conversations de manière intentionnelle et en divulgue les enregistrements vocaux à Nuance et « *qu'aucune exception ne permet à une entreprise d'enregistrer clandestinement des communications privées au domicile*[134] ».

3.3.1.2.3. La loi sur la protection de la vie privée des enfants en ligne

L'EPIC s'appuie également sur la loi sur la protection de la vie privée des enfants en ligne (*Children's Online Privacy Protection Act* – COPPA[135]) pour démontrer que la FTC est fondée à intervenir. La FTC est en effet habilitée à mettre en œuvre la COPPA, tout comme la loi relative à la FTC.

La COPPA a pour objectif de protéger la vie privée des enfants de moins de 13 ans en réglementant la collecte des informations personnelles relatives aux enfants par les opérateurs de sites web ou de services en ligne.

Les dispositions de la COPPA s'appliquent aux opérateurs de services en ligne, de sites web et d'applications destinés aux enfants de moins de 13 ans[136] – ainsi qu'aux opérateurs de services en ligne, de sites web et d'applications visant un public large qui ont effectivement connaissance du fait qu'ils collectent ou gèrent les informations personnelles d'un enfant[137]. Pour être en conformité avec cette loi, les opérateurs concernés doivent :

a) Avertir sur leur site web ou leur service en ligne du type d'informations relatives aux enfants qu'ils collectent, de la manière dont celles-ci sont utilisées, et de la manière dont ils divulguent ces informations[138] ;
b) Obtenir un consentement vérifiable des parents en amont de toute collecte, utilisation et/ou divulgation d'informations personnelles relatives aux enfants[139] ;

---

[129] *Electronic Communications Privacy Act* de 1986 (ECPA), 18 U.S.C. § 2510-2522.

[130] La définition de la « personne » inclut les entreprises ; 18 U.S.C. § 2510(6).

[131] 18 U.S.C. § 2511(1)(a).

[132] 18 U.S.C. § 2511(1)(c).

[133] *Op. cit.*, note de bas de page 112, paragraphe 71.

[134] *Ibid.* paragraphe 70.

[135] *The Children's Online Privacy Act* de 1998 (COPPA), 15 U.S.C. § 6501-6505.

[136] Title 16 of the Code of Federal Regulation (16 C.F.R.) §312.3.

[137] *Ibid*.

[138] 16 C.F.R. §312.4(b).

[139] 16 C.F.R. §312.5.

c) Mettre à disposition un moyen raisonnable pour que le parent soit en mesure de vérifier les informations personnelles collectées relatives à un enfant et de s'opposer à la poursuite de leur utilisation ou gestion[140] ;
d) Ne pas conditionner la participation d'un enfant à un jeu, l'octroi d'un prix, ou une autre activité à la communication de données personnelles excédant ce qui est raisonnablement nécessaire pour participer à une telle activité ;[141]
e) Etablir et maintenir des procédures raisonnables en vue de protéger la confidentialité, la sécurité et l'intégrité des données personnelles relatives aux enfants qui sont collectées[142].

L'EPIC tente d'abord d'établir que Samsung peut être qualifié de fournisseur de service en ligne, soumis aux obligations ci-dessus, en s'appuyant sur la politique de confidentialité complémentaire de Samsung en matière de téléviseurs connectés – la politique de confidentialité visant spécifiquement les téléviseurs connectés de Samsung. Cette politique de confidentialité complémentaire affirme : « *Les services de smart TV peuvent mettre à disposition des vidéos éducatives et d'autres contenus adaptés aux enfants, mais nous ne collectons délibérément aucune donnée personnelle relative aux enfants de moins de 13 ans sans consentement parental, sauf si la loi le permet*[143] ». Selon l'EPIC, Samsung se présente donc comme un opérateur de service en ligne visant un public global en conformité avec la COPPA.

Cependant, l'EPIC affirme que Samsung adapte spécifiquement certaines fonctionnalités des téléviseurs connectés aux jeunes enfants ; Samsung incite les parents à encourager leurs enfants à interagir avec les téléviseurs connectés Samsung et l'entreprise a reconnu que les téléviseurs connectés sont communément acquis par des familles comprenant des enfants de moins de 13 ans[144]. Sur cette base, l'EPIC conclut que Samsung enfreint la COPPA dans la mesure où il ne se conforme pas à la disposition 16 C.F.R. §312.3 – l'obligation de demander aux parents la permission d'enregistrer, de stocker et de transmettre les voix des enfants à une partie tierce.

3.3.1.2.4. La loi relative à la FTC

En vertu de la section 5 de la loi relative à la FTC, cette dernière est habilitée à prévenir les activités et pratiques déloyales et trompeuses[145]. Bien que cette loi ne donne pas à la FTC une autorité spécifique en matière de protection du droit à la vie privée, elle a été interprétée d'une façon qui a permis à la FTC de prévenir certaines intrusions dans la vie privée sur la base des dispositions en matière d'activités et pratiques déloyales et trompeuses[146].

L'EPIC décrit tant les pratiques déloyales que trompeuses des téléviseurs connectés Samsung, et analyse ainsi la loi relative à la FTC en lien avec les déclarations de principe de la FTC relatives au caractère trompeur[147] et déloyal[148].

---

[140] 16 C.F.R. §312.6.

[141] 16 C.F.R. §312.7.

[142] 16 C.F.R. §312.8.

[143] *Op. cit.*, note de bas de page 112, paragraphe 87 ; Politique de confidentialité globale de Samsung, complément relatif aux téléviseurs connectés https://www.samsung.com/uk/info/privacy-SmartTV.html?CID=AFL-hq-mul-0813-11000170.

[144] *Op. cit.*, note de bas de page 112, paragraphes 89-91.

[145] 15 U.S.C. § 45(a)(2).

[146] Electronic Privacy Information Center, *« Federal Trade Commission : Overview of Statutory Authority to Remedy Privacy Infringements »,* https://epic.org/privacy/internet/ftc/Authority.html.

[147] Federal Trade Commission, Déclaration de principe de la FTC sur le caractère trompeur, 1983, https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.

[148] Federal Trade Commission, Déclaration de principe de la FTC sur le caractère déloyal, 1980, https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.

Caractère déloyal

Une pratique commerciale est jugée déloyale lorsqu'elle « *cause ou est susceptible de causer un préjudice grave aux consommateurs qui ne peut être raisonnement évité par les consommateurs eux-mêmes et qui n'est pas compensé par des avantages pour les consommateurs ou la concurrence*[149] ».

Premièrement, la notion de « gravité » dans ce contexte porte habituellement sur un préjudice financier, mais elle peut également concerner des risques injustifiés pour la santé et la sécurité. L'existence de préjudices émotionnels et d'autres « types plus subjectifs de préjudices » ne signifient généralement pas que la pratique est déloyale[150].

S'agissant du deuxième élément, indiquant que le préjudice ne doit pas être compensé par des avantages pour les consommateurs ou la concurrence, la FTC détermine si « les effets nets d'une pratique sont dommageables[151] ».

En troisième lieu, la FTC examine si les consommateurs auraient pu raisonnablement éviter le préjudice en question.

L'EPIC affirme que le « préjudice grave » est avéré dans la mesure où Samsung n'assume pas la responsabilité pour le respect de la confidentialité et de la sécurité des conversations enregistrées des utilisateurs, ce qui entraîne que Samsung, « *de manière déraisonnable, crée ou tire avantage d'un obstacle à la possibilité pour le consommateur de prendre sa décision librement* »[152]. Pour établir ce préjudice, l'EPIC rappelle les tentatives de Samsung pour se dégager de sa responsabilité quant aux pratiques en matière de confidentialité et de sécurité des sociétés auxquelles il transfère les données qu'il a collectées à propos de ses utilisateurs, et le fait que Samsung transmet les conversations privées des utilisateurs de téléviseurs à la partie tierce Nuance[153]. En outre, l'EPIC se réfère à la politique de confidentialité de Samsung, qui ne révélait pas aux consommateurs le nom de l'entreprise tierce. Samsung a ensuite induit les consommateurs en erreur sur la question du recours au cryptage pour la transmission des conversations enregistrées, selon l'EPIC. De plus, l'EPIC affirme que cette absence de protections adéquates n'est pas compensée par des avantages pour les consommateurs ou la concurrence[154].

Enfin, l'EPIC avance que les utilisateurs des téléviseurs connectés Samsung n'étaient pas raisonnablement en mesure de prévoir qu'en utilisant les téléviseurs connectés, leurs conversations privées seraient communiquées, parfois sans qu'elles aient été cryptées, à Nuance[155]. L'EPIC conclut donc que le fait que Samsung n'a pas divulgué ces aspects de manière adéquate est constitutif d'une activité ou pratique déloyale[156].

Caractère trompeur

En vertu de la politique de la FTC en matière de pratiques trompeuses, une activité est considérée comme trompeuse si elle « *implique une déclaration, omission ou pratique qui est susceptible d'induire en erreur un consommateur agissant de manière raisonnable au vu des circonstances, au détriment de ce consommateur*[157] ». Le caractère trompeur est donc constitué de trois éléments.

D'abord, il doit exister une déclaration, omission ou pratique susceptible d'induire le consommateur en erreur. Les pratiques jugées trompeuses incluent des déclarations écrites fausses,

[149] 15 U.S.C. § 45 (n).

[150] *Op. cit.*, note de bas de page 148.

[151] *Ibid.*

[152] *Op. cit.*, note de bas de page 112, paragraphe 107.

[153] *Ibid.*, paragraphe 103.

[154] *Ibid.*, paragraphe 109.

[155] *Ibid.*, paragraphe 108.

[156] *Ibid.*, paragraphe 110.

[157] *Op. cit.*, note de bas de page 147.

des affirmations trompeuses sur les prix et le défaut de prestation des services promis[158]. Afin de déterminer le caractère trompeur de l'activité ou de la pratique, on examine si l'activité ou la pratique est susceptible d'induire en erreur, et non si l'activité ou la pratique a effectivement induit en erreur[159].

Deuxièmement, l'activité ou la pratique doit être considérée comme trompeuse du point de vue d'un consommateur agissant de manière raisonnable compte tenu des circonstances. La FTC examine l'activité ou la pratique dans son ensemble[160]. En troisième lieu, l'activité ou la pratique doit être « matérielle », c'est-à-dire qu'elle doit être susceptible d'affecter le comportement ou la décision du consommateur vis-à-vis du produit ou du service[161]. La FTC examinera donc si les consommateurs auraient choisi un autre produit, s'il n'y avait pas eu activité ou pratique trompeuse.

Selon l'EPIC, Samsung a agi de manière trompeuse en ne divulguant pas le fait qu'il enregistre et communique les conversations privées via ses téléviseurs connectés. L'EPIC avance que les consommateurs ont par conséquent été induits en erreur, puisqu'ils ne savaient pas que leurs conversations personnelles étaient effectivement enregistrées et transmises à une tierce partie. De plus, Samsung les a assurés du fait qu'il cryptait toutes les transmissions, alors que dans les faits, certains enregistrements vocaux étaient transmis sans cryptage. Lorsque les utilisateurs ont été informés de cette collecte et cette communication des données, ils s'y sont opposés et ont estimé qu'il s'agissait d'une pratique illégale, ce qui indique que le caractère trompeur était de nature « matérielle » du point de vue des consommateurs. L'EPIC conclut que les déclarations insuffisantes de Samsung constituent bien des activités ou pratiques trompeuses interdites par la disposition 15 U.S.C. § 45(a)[162].

3.3.1.3. Implications possibles

La FTC n'a pas, à ce jour, pris de mesures formelles contre Samsung. La réaction de la FTC dans cette affaire est susceptible d'avoir un impact important, en raison de l'émergence rapide des appareils interactifs en général, et de l'absence de jurisprudence sur la smart TV tant aux Etats-Unis qu'en Europe. Quelle que soit sa conclusion, cette affaire met en lumière des pistes intéressantes qui pourraient être suivies pour réglementer l'impact des téléviseurs connectés sur la vie privée. Les dispositions juridiques sur lesquelles la plainte de l'EPIC se fonde éclairent des voies possibles pour répondre à l'émergence des téléviseurs connectés ; en renforçant la protection des consommateurs par un accroissement de la transparence dans les politiques de confidentialité, ou en s'appuyant sur des lois spécifiques telles que la CCP et l'ECPA, qui concernent plus particulièrement les transferts illégaux de données personnelles.

Bien qu'il soit difficile de se prononcer sur l'issue possible de cette affaire, la présidente de la FTC, Mme Edith Ramirez, a récemment abordé dans un discours le problème spécifique des appareils qui espionnent les consommateurs, en se référant notamment aux téléviseurs connectés. Elle a déclaré que : « *l'application* de *limites raisonnables à la collecte et à la conservation des données constitue la première ligne de défense pour la vie privée du consommateur*[163] ». Sur la base

[158] *Ibid.*

[159] *Ibid.*

[160] *Ibid.*

[161] *Ibid.*

[162] *Op. cit.*, note de bas de page 112, paragraphe 102.

[163] Privacy and the Internet of Things: Navigating Policy Issues - *Opening Remarks of FTC Chairwoman Edith Ramirez,* International Consumer Electronics Show, Las Vegas, 6 janvier 2015.

de cette prise de position, il est probable que la FTC interviendra sur la question de l'impact des téléviseurs connectés sur la vie privée.

Plus récemment, l'EPIC a appelé la FTC et le département de la Justice à mener une enquête approfondie en vue de déterminer si les appareils « activés en permanence » enfreignaient la loi sur les écoutes (*Wiretap Act*), les lois fédérales en matière de vie privée, ou la loi relative à la FTC[164]. L'EPIC s'est à nouveau tournée vers la FTC dans l'objectif de protéger la vie privée des consommateurs dans le cadre de leur utilisation d'appareils interactifs.

[164] Voir https://epic.org/2015/07/epic-urges-investigation-of-al.html.

4. Le Règlement Général sur la Protection des Données

Ce chapitre vise principalement à fournir un aperçu du futur règlement général sur la protection des données (ci-après appelé « RGPD » ou « règlement »). Le processus législatif menant à l'adoption de ce nouveau texte n'est pas terminé, mais se trouve dans sa phase finale. Le 24 juin 2015, le Parlement européen, le Conseil et la Commission européenne ont entamé les négociations de codécision au sujet de la proposition de RGPD. Ces négociations se fondent sur la proposition de la Commission de janvier 2012, la résolution législative du Parlement du 12 mars 2014 et l'orientation générale du Conseil adoptée le 15 juin 2015[165]. Nous analyserons dans ce chapitre les principales différences entre l'applicabilité aux smart TVs de l'actuelle directive sur la protection des données et celle du futur RGPD[166]. La version définitive du règlement est attendue pour décembre 2015, ce qui pourrait conduire à son adoption officielle au début de l'année 2016[167].

4.1. Les Smart TVs et le Règlement Général sur la Protection des Données

Après avoir défini au chapitre I les smart TVs et le type de données qu'ils peuvent collecter, nous examinerons dans ce chapitre si ces données peuvent être considérées comme des données à caractère personnel aux fins du (projet de) RGPD.

[165] 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), COM(2012)11 final, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_fr.pdf ; résolution législative du Parlement européen du 12 mars 2014 sur 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),

www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//FR ; 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) – Préparation d'une orientation générale, document du Conseil 9565/15, 11 juin 2015, http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/fr/pdf.

[166] Sur la base du Document du Conseil 10391/15, du 8 juillet 2015, http://data.consilium.europa.eu/doc/document/ST-10391-2015-INIT/EN/pdf.

[167] Contrôleur européen de la protection des données, « Recommandations du CEPD relatives aux options de l'UE en matière de réforme de la protection des données », 2015/C301/01, 12 septembre 2015,

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-07-27_GDPR_summary_FR.pdf.

4.1.1. Définitions

Les définitions et la portée du règlement sont étroitement apparentées à celles de la directive sur la protection des données. Son champ d'application est détaillé dans l'article 2 (« Champ d'application matériel »), qui dispose que le règlement s'applique uniquement au traitement des données à caractère personnel. L'article pose les deux notions clés en matière de protection des données : le traitement et les données à caractère personnel. L'article 4 (« Définitions ») définit ces termes.

Le premier terme, « traitement », est défini de façon large, de sorte que toute action ou presque peut constituer un traitement. Malgré l'amendement proposé par le Parlement européen à sa définition, le champ d'application de l'article 2 du RGPD n'a pas été élargi pour s'étendre au traitement « quel que soit le moyen[168] » ; en conséquence, le règlement continue de s'appliquer au traitement de données à caractère personnel lorsqu'il est effectué en partie ou en totalité de façon automatisée[169].

L'ampleur du périmètre d'application de la directive sur la protection des données et, désormais, du règlement est notamment manifeste dans l'arrêt *Bodil Lindqvist*[170] qui examine la notion de traitement aux fins de la directive 95/46. Le raisonnement développé peut être transposé au règlement, puisque les définitions sont identiques dans les deux textes. En l'espèce, la CJUE a estimé que la mention du numéro de téléphone et des loisirs d'une personne sur un site web pouvait être considérée comme un traitement. Ce dernier n'était en outre pas entièrement automatisé : il est donc admis qu'un traitement automatisé en partie relève du champ d'application du règlement.

La notion de « données à caractère personnel » demeure également inchangée par rapport à la directive sur la protection des données. Les données à caractère personnel sont définies comme « toute information concernant une personne physique identifiée ou identifiable[171] ». On peut distinguer quatre éléments pertinents pour l'application de cette notion, à savoir, selon le groupe de travail « Article 29 » : 1) il peut s'agir de « toute information » ; 2) « concernant » ; 3) [une personne] « identifiée ou identifiable » ; 4) une « personne physique[172] ».

4.1.1.1. « Toute information »

L'emploi des termes « toute information » témoigne de l'intention du législateur de l'Union de conférer une acception large à la notion de données à caractère personnel. Les avis du groupe de travail « Article 29 » partent du principe que l'expression « toute information » recouvre les informations tant objectives que subjectives. Il n'est du reste pas nécessaire que ces informations soient vraies ou prouvées[173]. En outre, il est sans incidence que les informations aient trait aux activités professionnelles ou privées d'une personne. Dans les affaires jointes *Volker und Markus*

[168] Article 2 du RGPD, voir document du Conseil 10391/15 conformément à la Position du Parlement européen / Première lecture, *ibid.* note de bas de page 166, p 233.

[169] « Le présent règlement s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier. » (article 2, paragraphe 1, du RGPD).

[170] CJUE, affaire C-101/01, *Bodil Lindqvist,* 6 septembre 2003, http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:62001CJ0101.

[171] Article 4, paragraphe 1, du RGPD, document du Conseil 10391/15 conformément à l'Orientation générale du Conseil (15/06/2015), *op. cit.*, note de bas de page 166.

[172] Groupe de travail « Article 29 », avis 4/2007, *op. cit.*, note de bas de page 47.

[173] *Ibid*.

Schecke GbR et Hartmut Eifert c. Land Hessen[174], la CJUE a estimé que les activités professionnelles pouvaient également entrer dans le champ de la vie privée. Cette conclusion se retrouve également dans la jurisprudence de la Cour européenne des droits de l'homme, qui a opté pour une approche semblable dans l'arrêt *Amann c. Suisse*[175]. Le mode de stockage des données peut lui aussi constituer un facteur différenciateur : fichiers numériques, film, documents imprimés ou cassettes audio peuvent tous contenir des données à caractère personnel.

4.1.1.2. « Concernant »

Cet élément peut paraître évident au premier abord : après tout, les données doivent d'une façon ou d'une autre concerner une personne donnée pour être considérées comme des données à caractère personnel. La réalité est toutefois quelque peu plus nuancée. Le groupe de travail « Article 29 » énonce trois critères pour déterminer si les données « concernent » une personne : le contenu, la finalité et le résultat. Ils s'appliquent de façon non cumulative.

En résumé, les données dont le *contenu* a des répercussions pour une personne *concernent* donc cette personne. Des données concernent une personne lorsqu'elles peuvent être utilisées pour une *finalité* susceptible, par exemple, d'influer sur le comportement d'un individu. Enfin, les données qui peuvent être employées pour obtenir un *résultat* donné pour des personnes données peuvent être considérées comme concernant ces personnes.

4.1.1.3. « Une personne « identifiée ou identifiable »

La différence essentielle entre « identifiée » et « identifiable » réside dans le fait qu'une personne identifiable n'a pas encore été identifiée[176]. L'article 4, paragraphe 1, du règlement évoque la possibilité d'une identification directe ou indirecte[177]. L'identification directe est possible par exemple par l'intermédiaire du nom de la personne. L'identification via un identifiant personnel tel qu'un numéro de passeport ou de sécurité sociale constitue une forme d'identification indirecte, puisqu'il est nécessaire d'avoir recours à d'autres données ou à des moyens complémentaires pour déterminer l'identité de la personne concernée. Bien entendu, la possibilité d'identifier un sujet en recoupant plusieurs « identifiants » dépend des circonstances. L'identification indirecte peut être considérée comme un processus d'identification grâce à une série d'éléments qui permet de distinguer une personne au sein d'un groupe. Cela pose la question de savoir à quel moment l'on atteint le point d'identification indirecte, c'est-à-dire celui où un tiers dispose de suffisamment de raisons ou d'éléments pour identifier la personne concernée. Le règlement aborde la question au considérant 23, qui indique qu'il convient en la matière de considérer l'ensemble des moyens raisonnablement susceptibles d'être mis en œuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier directement ou indirectement l'individu[178]. Cet examen doit tenir compte de tous les facteurs pertinents, tels que le temps et l'effort nécessaires à l'identification, mais aussi les technologies les plus récentes et leur évolution.

---

[174] CJUE, affaires jointes C-92/09 et C-93/09, *Volker und Markus Schecke GbR et Hartmut Eifert c. Land Hessen*, 9 novembre 2010, http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:62009CJ0092.

[175] Arrêt de la Cour européenne des droits de l'homme, affaire *Amann c. Suisse*, *op. cit.*, note de bas de page 71.

[176] *Op. cit.*, note de bas de page 47.

[177] Article 4 paragraphe 1 du RGPD, document du Conseil 10391/15 conformément à l'Orientation générale du Conseil (15/06/2015), *op. cit.* note de bas de page 166.

[178] *Ibid.*

Le considérant 23 du RGPD permet en outre d'établir une distinction entre les données à caractère personnel et celles d'une autre nature[179]. Lorsque les données sont anonymes et qu'il n'est pas possible de retrouver à quelle personne elles se rapportent (grâce à leur agrégation, par exemple), elles ne constituent plus des données à caractère personnel, puisqu'elles ne peuvent plus être rattachées à la personne concernée.

4.1.1.4 « Personne physique »

Le dernier élément implique que les règles relatives à la protection des données s'appliquent en principe à toute personne vivante[180]. Quelques exceptions peuvent être détaillées, mais elles seraient d'un intérêt limité pour la présente étude.

4.1.1.5. Catégories particulières de données

Considérés conjointement, les éléments susmentionnés fournissent un cadre permettant de déterminer si certaines informations constituent des données à caractère personnel. A l'instar de la directive sur la protection des données, le règlement établit ensuite une distinction supplémentaire entre données « ordinaires » et catégories particulières de données. L'article 9 (« Traitement des catégories particulières de données à caractère personnel») énumère les types de données concernées : les données sur l'origine raciale ou ethnique, les opinions politiques, les croyances religieuses ou philosophiques, l'appartenance à un syndicat, et le traitement des données génétiques ou des données concernant la santé ou relatives à la vie sexuelle[181]. Dans le texte de première lecture de la Position du Parlement européen, les données biométriques et celles concernant les sanctions administratives, les jugements, les infractions pénales ou présumées pénales, ainsi que les condamnations sont également comprises[182]. De toute évidence, il s'agit là encore d'une sous-catégorie large. Un régime plus strict est mis en place pour cette catégorie spéciale de données. Il sera évoqué plus loin, mais pour l'heure, nous nous contentons de mentionner l'existence de cette catégorie distincte.

4.1.1.6. Champ d'application territorial

Outre le champ d'application matériel du règlement, l'article 3 (« Champ d'application territorial ») établit son applicabilité (extra-)territoriale[183]. Le paragraphe 1 dispose que le règlement s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement de données ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait ou non lieu dans l'Union. Le paragraphe 2 constitue l'un des apports nouveaux du règlement. Il prévoit que le règlement s'applique également si le sous-traitant n'est pas établi dans l'Union, lorsque les activités de traitement sont liées a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non de celles-ci ; ou b) à

[179] *Ibid.*, p 29-31.

[180] *Op. cit.*, note de bas de page 47.

[181] Document du Conseil 10391/15 conformément à l'Orientation générale du Conseil (15/06/2015), *Ibid.* note de bas de page 166.

[182] L'énoncé exact de cet article est encore controversé. Voir document du Conseil 10391/15 conformément à la Position du Parlement européen / Première lecture, *Ibid*. note de bas de page 166.

[183] Document du Conseil 10391/15, *Ibid.* note de bas de page 166.

l'observation de ces personnes concernées, dans la mesure où leur comportement a lieu dans l'Union. Ceci témoigne de l'intention du législateur d'élargir le champ du règlement, en comparaison de celui de la directive.

4.1.2. Application

Le champ d'application du règlement présenté ci-dessus peut englober les smart TVs, ainsi que nous l'avons expliqué au chapitre I. Dès lors que les données ne constituent pas des données à caractère personnel au sens du règlement, toutefois, les autres dispositions de ce dernier perdent toute pertinence. Nous allons à présent examiner les différentes fonctions décrites dans le chapitre I au regard de leurs conséquences juridiques.

4.1.2.1. Reconnaissance vocale

Ainsi que nous l'avons indiqué plus haut, une smart TV est en mesure d'enregistrer des sons émis à ses abords et de reconnaître des empreintes vocales, qui peuvent à leur tour être enregistrées comme des commandes vocales. On peut se demander si cette fonction entraîne le traitement de données à caractère personnel. La réponse varie selon les circonstances.

Il convient tout d'abord d'examiner le contenu des conversations susceptibles d'être ainsi enregistrées. Le téléviseur occupant généralement une place centrale dans le foyer, il est en mesure de capter un nombre considérable d'interactions vocales. Le contenu de ces conversations n'est bien sûr jamais le même et elles peuvent faire intervenir un nombre infini de combinaisons de mots. Sans aucun doute, on trouvera parmi ces derniers des noms de personnes et de lieux ainsi que d'autres renseignements permettant d'identifier des sujets. On y relèvera également une part de « bruit blanc », c'est-à-dire d'éléments qui ne contiennent pas de renseignements pertinents ou permettant d'identifier une personne.

Pour revenir aux critères énumérés dans le règlement, il convient de garder à l'esprit que la définition des données à caractère personnel évoque « toute » information concernant une personne physique. Par analogie, on peut faire référence à l'arrêt de la Cour suprême des Pays-Bas dans l'affaire *Dexia*[184], qui a estimé que les enregistrements de conversations téléphoniques pouvaient, à certaines conditions, être considérés comme des données à caractère personnel. Nous avons par ailleurs montré plus haut qu'il était relativement simple d'identifier indirectement une personne moyennant la collecte d'une quantité suffisante d'informations. Puisque les smart TVs ne font pas de distinction entre les sons à enregistrer ou non – il faut bien filtrer l'ensemble des sons afin de pouvoir reconnaître parmi eux les commandes vocales – il semble fondé de conclure que les sons captés dans les lieux de vie répondent à la définition des données à caractère personnel. Reste à savoir si leur enregistrement constitue un traitement. L'article 4, paragraphe 3, du règlement indique que le traitement recouvre la collecte, l'enregistrement, la conservation, l'utilisation et la transmission d'informations, que ces opérations soient effectuées ou non à l'aide de procédés automatisés. On peut donc affirmer que l'enregistrement du contenu de conversations constitue une forme de traitement de données à caractère personnel aux fins du règlement. Ce traitement peut également recouvrir des données à caractère personnel énumérées dans les catégories de l'article 9.

[184] Cour suprême des Pays-Bas, affaire *Dexia,* arrêt du 29 juin 2007, ECLI:NL:HR:2007:AZ4664, par. 3.8 et suivants, http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:HR:2007:AZ4664.

4.1.2.2. Commande gestuelle et reconnaissance faciale

Nous avons vu dans le chapitre I que les smart TVs étaient à même d'enregistrer des images et de reconnaître des visages. Si les enregistrements sonores relèvent du champ d'application du règlement, la même question peut être posée s'agissant de ces enregistrements visuels.

Les images requièrent une analyse plus fine que les sons. Les photos peuvent permettre l'identification directe des individus qu'elles montrent et les photos-portraits sont généralement traitées comme des données à caractère sensible, puisqu'elles permettent de déterminer certaines caractéristiques telles que l'appartenance ethnique.

L'examen du règlement, à cet égard, est sans surprise, puisque les images des personnes constituent des informations relatives à des personnes physiques identifiées ou identifiables. Elément non pris en compte dans la partie précédente concernant les enregistrements sonores : la possibilité que *toute personne* à proximité de l'appareil puisse être enregistrée. Les images et les sons peuvent en outre se rapporter à des mineurs ou à des visiteurs du foyer, et non aux utilisateurs habituels ou enregistrés. Dans pareil cas, le statut à part des mineurs ou des visiteurs entraînerait un scénario juridique particulier.

Comme dans le cas du son, l'enregistrement de ces informations visuelles constitue un traitement. On peut donc en conclure que la commande gestuelle et la reconnaissance faciale relèvent du champ du règlement.

4.1.2.3. Création d'un compte

Cette catégorie de données résiduelle englobe l'ensemble des données ne constituant pas des enregistrements visuels ou sonores. Il ne s'agit toutefois pas de donner l'impression que cette catégorie est d'une importance moindre. Au contraire, dans le cadre de la présente étude, ce qui suit est d'une importance primordiale.

Nous étudierons tout d'abord les informations pouvant être rattachées à un compte d'utilisateur, même s'il convient de préciser que de nombreux utilisateurs n'emploient pas un tel compte. Dans une moindre mesure, ce point s'applique aussi aux commandes vocales et gestuelles. Cependant, cette catégorie résiduelle comporte aussi des données qui s'appliquent à tous les utilisateurs et ont donc des incidences importantes pour ce rapport.

La création d'un compte requiert la saisie d'informations telles que le nom, l'adresse de messagerie électronique, la date de naissance et le code postal de l'utilisateur. A l'évidence, le nom constitue une donnée à caractère personnel. Bien que les autres données ne répondent pas nécessairement, en tant que telles, à la définition des données à caractère personnel, elles peuvent être croisées en vue d'identifier un individu. En conséquence, les informations saisies dans un compte constituent sans ambiguïté une forme de données à caractère personnel.

Examinons à présent le cas de figure dans lequel un utilisateur choisit de ne pas créer un compte. Après le tollé soulevé par les conditions d'utilisation des smart TVs de Samsung, le géant de la technologie n'a eu qu'un bref moment de répit : la controverse initiale a rapidement été suivie d'un article de presse accusant l'entreprise de diffuser des publicités dans les contenus visionnés par les utilisateurs sur leur réseau domestique[185]. Il ne s'agissait pas de contenus consultés en *streaming* ou téléchargés, mais achetés indépendamment par l'utilisateur. Samsung a réagi sans attendre et publié des excuses officielles indiquant que cet incident était le fruit d'une erreur. En tout état de cause, cet épisode prouve que l'ajout de publicités dans des contenus locaux est au moins

[185] Roettgers J., « Samsung TVs start inserting ads into your movies », *Gigaom*, 10 février 2015, https://gigaom.com/2015/02/10/samsung-tvs-start-inserting-ads-into-your-movies/.

techniquement possible. En outre, l'une des options des smart TVs permet d'afficher des contenus en fonction de l'historique de visionnage de l'utilisateur. Il n'est donc pas inconcevable que cet historique soit également utilisé en vue de proposer des publicités ciblées et des contenus personnalisés, ce qui se fait déjà sur de nombreux sites web[186].

Il n'est pas étonnant que les données collectées soient exploitées pour analyser le comportement de l'utilisateur, comme en témoignent les évolutions en matière de marketing en ligne de la décennie écoulée. La généralisation des *cookies* de suivi, de la collecte de l'« empreinte digitale » des navigateurs et du ciblage comportemental montre qu'il existe une demande considérable d'informations concernant les centres d'intérêt et les préférences des internautes[187]. Sans surprise, certains acteurs tentent de reproduire l'opération avec les smart TVs.

Avant de revenir à la définition des données à caractère personnel, arrêtons-nous sur le type de données qui sont effectivement collectées. Afin d'être à même de suggérer d'autres contenus, les smart TVs doivent pouvoir enregistrer le comportement du téléspectateur. D'un point de vue technique, il est tout à fait envisageable que soient ainsi enregistrés la durée et l'heure du visionnage, l'identité du téléspectateur et le mode de réception du programme (radiodiffusion, *streaming* ou sources émanant du réseau local). L'adresse IP du téléviseur peut fournir une localisation approximative. Il est également possible que le téléviseur retienne l'application utilisée pour se procurer le contenu, par exemple une application Netflix. Dans ce cas, Samsung *et* Netflix peuvent avoir intérêt à enregistrer ces informations. Une question annexe – mais intéressante – est celle de la façon dont ces applications sont présentées sur l'écran et comment est déterminé leur classement ou leur ordre d'apparition. Les questions liées à la notoriété ou à la visibilité des contenus seraient toutefois hors sujet ici.

Toutes ces catégories contiennent-elles des informations relatives à une personne physique identifiée ou identifiable ? En l'absence de création de compte, il n'y a pas de raison de penser qu'elles concernent une personne identifiée. Reste l'hypothèse d'une personne identifiable. Ainsi que nous l'avons établi plus haut, ce critère dépend des moyens par lesquels il est raisonnablement possible que la personne concernée puisse être identifiée. En tout état de cause, le sous-traitant concerné dispose d'informations quant au contenu visionné, à l'heure et à la durée de visionnage, ainsi qu'à l'application utilisée ; il peut en outre déterminer approximativement la localisation de l'utilisateur grâce à l'adresse IP utilisée[188].

La réponse varie naturellement au cas par cas. Cependant, au vu de la variété des émissions télévisées, programmes en *streaming* et autres contenus à disposition, ces informations devraient rapidement être en nombre suffisant pour rendre l'utilisateur identifiable. Pour reprendre les termes du règlement, ces renseignements permettent de tirer des conclusions à propos de l'identité sociale, psychique et culturelle de la personne concernée. Il s'ensuit que même lorsqu'une smart TV n'est pas muni d'une caméra et d'un microphone, et en l'absence de compte personnel créé par l'utilisateur, un traitement de données à caractère personnel peut tout de même avoir lieu. Ainsi que nous l'avons expliqué au chapitre III, les études réalisées par l'Autorité néerlandaise de protection des données ont permis de conclure que les informations contenues dans un historique

---

[186] Titlow J. P., « How Yahoo's homepage delivers personalized news to 700 million people », *ReadWrite*, 10 février 2012, http://readwrite.com/2012/02/10/how_yahoos_homepage_delivers_personalized_news_to.

[187] Zuiderveen Borgesius F. J., « Behavioural Sciences And The Regulation Of Privacy On The Internet », rapport de recherche de la faculté de droit de l'université d'Amsterdam, n° 2014-54, p. 3 et suivantes, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2513771.

[188] La question de savoir si une adresse IP constitue en elle-même une donnée à caractère personnel fait actuellement l'objet d'une demande de décision préjudicielle adressée à la CJUE dans l'affaire C-582/14, *Breyer c. République fédérale d'Allemagne*, http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:62014CN0582. Le groupe de travail « Article 29 » considère d'ores et déjà que les adresses IP sont une forme de données à caractère personnel. Voir son avis 01/2012 sur les propositions de réforme de la protection des données adopté le 23 mars 2012,

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_fr.pdf. Le projet de règlement proprement dit se contente d'une référence ambiguë aux adresses IP dans le considérant 24.

de visionnage pouvaient avoir des incidences non négligeables sur le droit au respect de la vie privée, de sorte qu'il est possible de les considérer comme des données à caractère sensible[189]. Avec la possibilité accrue de sélectionner nos propres contenus grâce à la télévision à la demande, il est plus intéressant et plus facile de déterminer les préférences de chacun sur la base de leurs habitudes de téléspectateur.

4.2. Degré de protection offert par le règlement

Après avoir examiné, dans la partie précédente, si les smart TVs relevaient dans la plupart des cas du champ d'application du règlement et avoir conclu par l'affirmative, nous étudierons ici les garanties offertes par le règlement, sur la base des mêmes scénarios. Il n'est pas dans notre intention de passer en revue de façon exhaustive toutes les dispositions du règlement. Nous nous attarderons sur celles qui ont trait aux questions juridiques soulevées dans le chapitre III, ce qui nous renseignera quant au degré de protection offert par le texte et nous permettra d'approfondir ensuite son évaluation.

4.2.1. Dispositions clés

Dans le chapitre II du règlement, l'article 5 pose les mêmes principes que l'article 6 de la directive 95/46/CE, mais sous une forme plus spécifique et moyennant quelques ajouts[190]. Nous verrons plus en détail ci-dessous que la notion de consentement y est définie de façon plus précise. Comme nous l'avons évoqué dans le chapitre II, ces principes établissent les limites de ce qui constitue un traitement légitime des données. Ils constituent donc en tant que tels un cadre de référence pour les autres dispositions et sont essentiels à la bonne compréhension du système mis en place par le règlement.

Appliqués au scénario qui nous est désormais familier, ces principes nous renseignent sur la façon dont Samsung devrait aborder les données à caractère personnel collectées. Il n'est pas possible de procéder à une analyse plus spécifique, en l'absence d'informations complémentaires concernant les actions de traitement réellement effectuées. L'approche de Samsung sert ici d'illustration et prépare les développements qui suivent.

L'article 6 du règlement définit les bases sur lesquelles doit reposer la licéité du traitement. Selon cette méthode, déjà présente dans la directive, tout acte de traitement de données doit correspondre à l'une au moins des situations suivantes :

> *« a) la personne concernée a consenti sans ambiguïté au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ;*
>
> *b) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;*
>
> *c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;*
>
> *d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne ;*

[189] Autorité néerlandaise de protection des données, *op. cit.*, note de bas de page 109.

[190] Document du Conseil 10391/15, *op. cit.*, note de bas de page 166.

e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;

f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant[191] *(…). »*

Parmi les critères susmentionnés, trois présentent une importance particulière pour notre scénario, ainsi qu'en témoigne l'arrêt *TP-Vision*[192] : a) le consentement, b) les obligations contractuelles et f) l'intérêt légitime du responsable du traitement[193]. Nous allons à présent voir si ces conditions peuvent servir de base aux actes de traitement décrits au chapitre III.

4.2.1.1. Obligations contractuelles

Au premier abord, ce motif peut apparaître comme une méthode évidente de légitimer un traitement de données. Après tout, Samsung pourrait tout simplement demander l'autorisation de traiter les données de ses clients dans ses contrats de vente, comme le prévoit l'article 7, point b), de la directive sur la protection des données. Toutefois, le groupe de travail « Article 29 » donne une interprétation très restrictive de cette disposition :

« La disposition doit être interprétée de façon restrictive et ne couvre pas les situations dans lesquelles le traitement n'est pas véritablement nécessaire à l'exécution d'un contrat, mais plutôt imposé unilatéralement à la personne concernée par le responsable du traitement[194]*. »*

En somme, le traitement doit être *essentiel* à l'exécution du contrat. L'Autorité néerlandaise de protection des données a en outre estimé, dans l'affaire *TP-Vision*, qu'il était « nécessaire de justifier le traitement en lien avec la personne concernée[195] ». L'achat de smart TVs repose essentiellement sur un contrat de vente qui a peu ou rien à voir avec le traitement de données à caractère personnel visuelles ou sonores. Cette disposition est en conséquence moins applicable qu'on ne pourrait le penser à première vue.

4.2.1.2. Intérêts légitimes du responsable du traitement

Lorsque ce motif est invoqué, il convient de mettre en balance l'intérêt du responsable du traitement et les droits fondamentaux de la personne concernée. Selon le groupe de travail « Article 29 », les « intérêts légitimes poursuivis par le responsable du traitement » peuvent être de

---

[191] Article 6 paragraphe 1 du RGPD, voir document du Conseil 10391/15, conformément à l'Orientation générale du Conseil (15/06/2015), *Ibid.*, note de bas de page 166.

[192] Autorité néerlandaise de protection des données, *op. cit.*, note de bas de page 109. Groupe de travail « Article 29 » sur la protection des données, Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/45/CE, 9 avril 2014,

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_fr.pdf.

[193] Parmi ces conditions, le consentement est l'élément le plus souvent invoqué dans les faits. Voir « Article 29 », avis 06/2014, *op. cit.*, note de bas de page 54 et suivantes.

[194] *Ibid.*

[195] Autorité néerlandaise de protection des données, *op. cit.*, note de bas de page 109.

nature variée[196]. En dernier ressort, la comparaison entre les intérêts du responsable du traitement et ceux de la personne concernée doit déterminer lesquels prévalent. Le considérant 38 fournit des précisions à ce sujet. Il indique qu'en sus des droits et libertés fondamentaux de la personne concernée, ses attentes raisonnables doivent également être prises en compte. Toutefois, ainsi que nous l'avons signalé plus haut, l'article 7, point f), de la directive sur la protection des données a connu d'importantes modifications en ce qui concerne la protection des mineurs. Lorsque la personne concernée est un enfant, il est peu probable que l'intérêt légitime du responsable du traitement supplante celui de l'enfant[197].

Cette disposition a été fréquemment critiquée dans le cadre de la directive sur la protection des données, car elle peut donner lieu à des interprétations variées. Cela demeure le cas, là encore. Parmi les reproches qui lui sont adressés figure le fait que la mise en balance des intérêts ne peut être effectuée que lorsque le traitement a déjà eu lieu, c'est-à-dire une fois que les pratiques de traitement déraisonnables ont été découverte et qu'un tribunal a été saisi pour procéder à cette évaluation[198].

Dans le cas des smart TVs, l'intérêt de Samsung réside essentiellement dans la fourniture d'une plateforme publicitaire de services et de contenus (y compris fournis par des tiers). C'est particulièrement vrai lorsqu'il est question d'analyser le comportement du téléspectateur. Les attentes raisonnables de l'acheteur reposent en grande partie sur les spécifications techniques du téléviseur proprement dit. Bien entendu, les fonctions « intelligentes » peuvent également influer sur les attentes, même s'il est peu probable que les utilisateurs s'attendent à ou souhaitent voir des publicités reposant sur leur comportement.

Il n'est pas toujours simple de mettre en balance les droits fondamentaux et les libertés de la personne concernée, d'une part, et les intérêts de Samsung, de l'autre. Un facteur important réside dans la place centrale qu'occupent souvent les téléviseurs au domicile des utilisateurs, un lieu où ces derniers sont particulièrement fondés à objecter à la surveillance et aux incursions dans la vie privée. L'utilisation de la télévision et la sélection des contenus sont également importantes ici. En évaluant les intérêts des parties dans l'affaire *TP-Vision*, l'Autorité néerlandaise de protection des données a tranché en faveur de la protection des personnes concernées.

4.2.1.3. Consentement

Ainsi que nous l'avons vu précédemment, le consentement est la justification la plus souvent avancée et selon l'Autorité néerlandaise de protection des données, c'est la seule qui vaille en matière de traitement des données par les smart TVs[199]. Ceci explique peut-être aussi pourquoi le législateur européen a décidé d'instaurer des garanties supplémentaires dans le règlement. Son article 4, paragraphe 8, définit le consentement comme suit :

> *« "consentement de la personne concernée" : toute* ***manifestation*** *de volonté, libre, spécifique et informée (...) par laquelle la personne concernée accepte, par une déclaration ou par un acte positif univoque, que des données à caractère personnel la concernant fassent l'objet d'un traitement.*[200] *»* (soulignement ajouté)

---

[196] Groupe de travail « Article 29 », avis 06/2014, *op. cit.*, note de bas de page 54.

[197] Article 6, point f) du RGPD, voir document du Conseil 10391/15 conformément à l'Orientation générale du Conseil (15/06/2015), *op. cit.*, note de bas de page 166.

[198] Bits of Freedom, *A loophole in data processing,* 2012, www.bof.nl/live/wp-content/uploads/20121211_onderzoek_legitimate-interests-def.pdf.

[199] *Ibid.*; Autorité néerlandaise de protection des données, *op. cit.*, note de bas de page 109.

[200] Document du Conseil 10391/15, conformément à l'Orientation générale du Conseil (15/06/2015), *op. cit.*, note de bas de page 166.

En vertu de la directive sur la protection des données, le consentement explicite de l'intéressé(e) n'est requis que pour le traitement des catégories spéciales de données à caractère personnel. Le projet de RGPD a introduit l'examen de ce critère comme une obligation générale pour apprécier l'octroi du consentement, mais celui-ci n'a pas été repris par le Conseil[201]. D'autre part, cette formulation montre que le consentement ne peut pas être donné implicitement, puisqu'elle évoque une « déclaration » ou un « acte positif univoque ».

L'article 7 du RGPD complète la directive sur la protection des données en détaillant les conditions du consentement. Il prévoit qu'en la matière, la charge de la preuve incombe au responsable du traitement[202]. En outre, lorsque le consentement est requis dans le contexte d'une déclaration écrite qui concerne également d'autres affaires, la demande relative au consentement doit être présentée sous une forme qui la distingue clairement de ces autres affaires[203]. L'article 7 permet également aux personnes concernées de retirer leur consentement à tout moment ; le retrait du consentement doit être aussi simple que son recueil. Le cas échéant, la personne concernée doit également être informée si le retrait du consentement peut mettre fin aux services fournis par le responsable du traitement[204]. Enfin, ainsi que nous l'avons indiqué au chapitre II, l'article 7 dispose que le consentement est limité à une finalité précise et devient caduc lorsque celle-ci n'existe plus ou dès lors que le traitement des données à caractère personnel n'est plus nécessaire pour la réalisation de la finalité pour laquelle elles ont été initialement collectées[205]. Il est significatif que la dernière phrase du paragraphe indique que l'exécution d'un contrat ou la fourniture d'un service ne doit pas être soumise à la condition préalable du consentement au traitement des données qui ne sont pas nécessaires à l'exécution du contrat ou à la fourniture du service.

Telles sont les conditions auxquelles Samsung doit satisfaire si l'entreprise souhaite procéder au traitement de données à caractère personnel sur la base du consentement. Elle doit recueillir le consentement des personnes concernées de telle façon qu'elles sachent clairement à quoi elles consentent. Samsung doit également préciser la nature des données traitées. Une étude réalisée en 2014 montre que tel n'est pas toujours le cas[206] ; elle conclut que les politiques de confidentialité des différents smart TVs ne couvrent pas toutes les finalités de traitement et que la demande de consentement est formulée en des termes extrêmement ambigus.

4.2.2. Autres dispositions pertinentes

Nous étudierons dans cette partie les autres dispositions susceptibles de peser sur le degré de protection des utilisateurs. L'article 8 (« Conditions applicables au consentement des enfants en ce qui concerne les services de la société de l'information ») prévoit des garanties supplémentaires pour le traitement des données relatives aux mineurs de moins de 13 ans[207]. Le traitement n'est alors licite que si et dans la mesure où le consentement est donné ou autorisé par un parent de

[201] *Ibid.*

[202] Article 7, paragraphe 1, du RGPD, voir document du Conseil 10391/15, conformément à l'Orientation générale du Conseil (15/06/2015), *op. cit.*, note de bas de page 166.

[203] Article 7, paragraphe 2, du RGPD, *ibid.*

[204] Article 7, paragraphe 3, du RGPD, *ibid.*

[205] Article 7 paragraphe 4 du RGPD, document du Conseil 10391/15, conformément à la Position du Parlement européen / Première lecture, *ibid.*

[206] Schermer B. V. et Falot N., *Analyse privacyvoorwaarden Smart TV*, 2014, www.considerati.com/wp-content/uploads/2014/09/201400820Onderzoek_privacyvoorwaarden_smarttv.pdf.

[207] Document du Conseil 10391/15, conformément à l'Orientation générale du Conseil (15/06/2015), *op. cit.*, note de bas de page 166.

l'enfant ou par son tuteur légal. En outre, le responsable du traitement doit s'efforcer raisonnablement de vérifier, en pareil cas, que le consentement est donné ou autorisé par le titulaire de la responsabilité parentale, compte tenu des moyens technologiques disponibles[208]. Dans le cas de Samsung, cela signifie que l'autorisation devrait être demandée au stade de l'installation, sans quoi (ainsi que nous l'avons établi dans le chapitre II), des données à caractère personnel relatives à des enfants pourraient faire l'objet d'un traitement. C'est aussi ce qui ressort clairement de l'argumentation dans les plaintes déposées par l'EPIC auprès de la FTC[209].

Puisque les données à caractère personnel relevant des « catégories spéciales » peuvent également faire l'objet d'un traitement au moyen de fonctions de reconnaissance faciale, il est intéressant de nous arrêter sur l'article 9 (« Traitement des catégories particulières de données à caractère personnel[210] »). Ces catégories bénéficient de garanties supplémentaires, comme le prévoit déjà l'article 8 de la directive sur la protection des données. Selon le paragraphe 2, elles ne peuvent faire l'objet d'un traitement qu'avec le consentement de la personne concernée. Ce consentement doit répondre à la définition évoquée précédemment. A titre d'exception, quelques motifs supplémentaires sont énumérés, mais ils sont d'une pertinence limitée pour le présent rapport. Pour notre étude de cas, cela pourrait signifier que le consentement est nécessaire avant l'activation des applications de reconnaissance faciale.

Conformément à l'article 14 (« Informations à fournir lorsque des données sont collectées auprès de la personne concernée »), le responsable du traitement est tenu de fournir diverses informations à la personne concernée[211]. L'article énumère les informations qui doivent être indiquées clairement à celle-ci. Il est permis de considérer qu'il s'agit là d'une série d'exigences pertinentes pour les futures politiques relatives au respect de la vie privée. Point essentiel, l'identité du responsable du traitement doit être communiquée à la personne concernée, de même que les finalités du traitement, la durée pendant laquelle les données à caractère personnel seront conservées, ainsi que les droits de ladite personne. Il ne s'agit pas là d'une évolution récente, bien que les conclusions du chapitre II montrent que ce point n'est pas toujours respecté dans les faits.

Le « droit à l'oubli », tel qu'il a été reconnu dans l'affaire *Google Spain*[212], a également été intégré dans le règlement. Il est évoqué ici pour ses liens étroits avec l'octroi du consentement et le droit corollaire de retrait. Ce dernier est garanti par l'article 17 (« Droit à l'effacement et à l'oubli numérique») et accorde à la personne concernée le droit d'obtenir du responsable du traitement l'effacement des données à caractère personnel la concernant[213]. Il peut être invoqué, notamment, lorsque les données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées, ou lorsque la personne concernée retire son consentement.

Les propriétaires de smart TVs peuvent ainsi demander l'effacement des données collectées à leur sujet lorsqu'ils décident de cesser d'utiliser l'appareil. Ceci leur confère un certain contrôle sur les informations qui les concernent.

Deux dispositions présentent une pertinence particulière pour notre scénario, les articles 19 (« Droit d'opposition ») et 20[214] (« Profilage »). Elles permettent aux utilisateurs de s'opposer aux pratiques de « profilage », définies comme suit dans l'article 4, paragraphe 3 *bis* :

> *« "profilage" : toute forme de traitement automatisé de données à caractère personnel destiné à évaluer certains aspects personnels propres à une personne physique ou à analyser*

[208] Article 8 du RGPD, *ibid.*

[209] EPIC, *op. cit.*, note de bas de page 112.

[210] Document du Conseil 10391/15, conformément à l'Orientation générale du Conseil (15/06/2015), *op. cit.*, note de bas de page 166.

[211] *Ibid.*

[212] CJUE, affaire C-131/12, *op. cit.*, note de bas de page 45.

[213] Document du Conseil 10391/15, conformément à l'Orientation générale du Conseil (15/06/2015), *op. cit.*, note de bas de page 166.

[214] *Ibid.*

ou prévoir en particulier le rendement professionnel de celle-ci, sa situation économique, sa localisation, son état de santé, ses préférences personnelles, sa fiabilité ou son comportement. »

L'analyse de l'historique de visionnage du téléspectateur par les fournisseurs de smart TVs semble correspondre à cette définition, puisqu'elle suppose une évaluation des préférences personnelles et du comportement. Cette interprétation est confirmée par les conclusions de l'Autorité néerlandaise de protection des données dans l'affaire *Ziggo.* Il s'agit d'une disposition qui vise les techniques de « ciblage comportemental » mises en œuvre par certains acteurs du marché. Conformément à l'article 19, les personnes concernées peuvent refuser ce type de profilage. En outre, en vertu de l'article 20, paragraphe 1 a), ces techniques ne peuvent être utilisées que si elles sont nécessaires à l'exécution d'un contrat, lorsqu'elles sont autorisées par la législation de l'Union ou d'un Etat membre, ou lorsqu'elles sont fondées sur le consentement de la personne concernée. Si Samsung ou Netflix souhaite analyser le comportement du téléspectateur, l'entreprise doit pouvoir justifier de l'un de ces motifs. Deux possibilités sont envisageables : recueillir le consentement de l'intéressé(e) ou passer par des contrats dans lesquels Samsung ou Netflix s'engage à fournir des suggestions de contenus sur la base du comportement du téléspectateur.

Autre disposition notable, l'article 23[215] (« Protection des données dès la conception et protection des données par défaut ») crée pour les responsables du traitement et les sous-traitants un devoir de mettre en œuvre des mesures et procédures techniques et organisationnelles appropriées et proportionnées, compte étant tenu des techniques les plus récentes, des connaissances techniques actuelles, des meilleures pratiques internationales et des risques représentés par le traitement des données. Eu égard aux conclusions du chapitre II, cela signifie que les responsables du traitement sont tenus de prendre des mesures supplémentaires afin de faire en sorte que leurs produits soient conformes aux spécifications applicables et de concevoir des interfaces compatibles. L'article 79 paragraphe 2 a) et e) cite la protection des données dès la conception et par défaut comme l'un des critères à considérer pour décider de l'application d'amendes administratives et du montant de celles-ci. En outre, ces amendes sont susceptibles d'atteindre un million d'euros ou 2 % du chiffre d'affaires annuel mondial de l'entreprise, une mesure qui pourrait faciliter l'exécution du texte[216]. Ce relèvement du plafond applicable aux amendes administratives devrait inciter fortement les multinationales à respecter les dispositions en vigueur.

La licéité des transferts de données internationaux constitue un autre sujet intéressant. Dans l'affaire *TP Vision*, les données étaient conservées sur place, aux Pays-Bas, mais il arrive bien sûr qu'un fournisseur choisisse de les transférer vers d'autres pays. Cette question est réglementée par les articles 41 à 45 *bis*[217]. L'article 41 autorise les transferts vers des pays tiers moyennant une décision officielle « relative au caractère adéquat du niveau de protection ». L'article 42 autorise également ces transferts lorsqu'il peut être établi que le pays de destination offre les garanties nécessaires. Enfin, en vertu de l'article 43, les responsables du traitement peuvent justifier le transfert à des pays tiers en souscrivant à des « règles d'entreprise contraignantes » (REC).

Il s'avère que le système mis en place par la directive pour réglementer les transferts vers les pays tiers était trop restrictif et trop exigeant, puisque les transferts internationaux à grande échelle avaient souvent lieu à l'intérieur des entreprises elles-mêmes. Un article décrit la nouvelle approche

[215] *Ibid.*

[216] Voir l'article 79, paragraphe 3, point a), voir Document du Conseil 10391/15, conformément à l'Orientation générale du Conseil (15/06/2015), *op. cit.*, note de bas de page 166.

[217] Document du Conseil 10391/15, conformément à l'Orientation générale du Conseil (15/06/2015), *op. cit.*, note de bas de page 166.

du règlement comme suit : « Concernant le problème des transferts structurels de données à caractère personnel au sein des multinationales, le projet offre à tout le moins des éclaircissements en codifiant des règles propres aux REC qui se sont développées sur le terrain. Partant du principe que les responsables du traitement appliquent également des REC, le texte rend possibles la délocalisation et le *cloud computing* vers des pays tiers. Il reste toutefois encore à préciser la façon dont les responsables du traitement sont censés utiliser ces REC.

Pour finir, le projet ne propose pas de solution au problème des demandes de données par des autorités gouvernementales de pays tiers. Au vu du processus de mondialisation en cours, de l'intensification des flux de données et des risques y afférents pour la protection des données à caractère personnel, il est essentiel que les nouvelles règles relatives aux transferts soient repensées et améliorées, de façon à ce qu'elles offrent un cadre viable et pérenne pour le traitement international des données et la protection des personnes concernées[218]. »

Il en ressort que les règles relatives aux transferts internationaux ont été clarifiées dans certains domaines. Bien que le règlement puisse offrir un surcroît de sécurité juridique concernant les transferts de données à caractère personnel transfrontières, le récent arrêt de la CJUE dans l'affaire *Maximillian Schrems c. Data Protection Commissioner* va plutôt dans le sens inverse[219].

4.3. Quel est le degré de protection adéquat et est-il assuré par le règlement ?

Nous avons jusqu'ici étudié la définition des smart TVs et les données qu'ils sont susceptibles de collecter, ainsi que le champ d'application du règlement et les garanties qu'il offre. Dans cette partie, nous examinerons les exigences nécessaires à une protection adéquate des utilisateurs de smart TVs, avant de procéder à une évaluation critique du règlement à cet égard.

4.3.1. Que protéger et pourquoi ?

La notion de degré de protection adéquat présuppose l'existence d'un objet à protéger. Il nous faut donc préciser *ce* qui est protégé, afin d'étudier les *raisons* pour lesquelles cette protection est indispensable. Sans cette étape, le raisonnement serait dénué de fondement.

En dernier ressort, les objets à protéger sont le droit au respect de la vie privée et familiale (article 7 de la Charte des droits fondamentaux de l'Union européenne) et le droit à la protection des données à caractère personnel (article 8). Il est toutefois instructif d'examiner pourquoi l'espace physique « occupé » par les smart TVs mérite d'être préservé, l'objet à protéger étant l'espace de liberté créé au sein du domicile. Cette opinion découle du champ d'application de l'article 7 de la charte, qui concerne « [la] vie privée et familiale, [le] domicile et [les] communications ». L'espace de liberté dont il est question sert à mener de nombreuses activités, et notamment à regarder la télévision, une occupation répandue à grande échelle, sur toute la planète. Elle est pratiquée pour différentes raisons, principalement à des fins de divertissement et d'acquisition de connaissances. Ces objectifs étaient autrefois réalisés grâce aux téléviseurs « bêtes », qui ne pouvaient diffuser que

[218] Wisman N. et de Vries H. H., *Doorgifte van persoonsgegevens onder de nieuwe Verordening*, P&I, 2012, p. 117, www.recht.nl/vakliteratuur/staatsrecht/artikel/358929/doorgifte-van-persoonsgegevens-onder-de-nieuwe-verordening/.

[219] Dans cette affaire, la Cour a invalidé la décision de la Commission relative à la « sphère de sécurité ». Pour de plus amples informations, voir http://curia.europa.eu/juris/celex.jsf?celex=62014CJ0362&lang1=en&type=TXT&ancre=; CJUE, affaire C-362/14, *op. cit.*, note de bas de page 56.

des images. Ainsi que nous l'avons évoqué plus haut, la situation a radicalement changé avec l'arrivée des smart TVs. Le téléspectateur peut soudain être observé chez lui et risque en conséquence de se mettre à adapter son comportement, consciemment ou non. Cela ne devrait pas être le cas dans un espace censé être libre, où l'on peut visionner des contenus et accéder à des informations en fonction de ses préférences personnelles. L'objet protégé devrait donc être l'espace dans lequel l'on peut, en somme, « être soi-même ». Julie Cohen a formulé ce point de vue de façon plus précise :

> *« Il existe un présupposé fondamental à notre discours concernant les activités de lecture, de pensée et d'expression : les individus dans notre société doivent se voir garantir la liberté de se former une réflexion et une opinion en privé, sans subir la surveillance intrusive d'entités gouvernementales ou privées*[220]*. »*

Si Julie Cohen s'intéresse ici à la lecture, le même raisonnement s'applique au visionnage de contenus, car ces deux façons d'emmagasiner des informations ne diffèrent pas fondamentalement. L'auteure répond aussi en partie à la question de savoir *pourquoi* une protection est nécessaire, en évoquant le premier amendement de la Constitution des Etats-Unis qui consacre la conception américaine de la liberté d'expression. Neil Richards argumente également en faveur du respect de la vie privée au domicile, en vertu de la liberté d'expression :

> *« Nous avons tendance à penser que les règles relatives au respect de la vie privée sont en conflit avec le premier amendement, mais il en va autrement de la protection de la vie privée intellectuelle. Il s'agit d'une composante vitale dans une culture bien ancrée de liberté d'expression, car elle garantit l'intégrité de nos activités intellectuelles en les protégeant des regards importuns et des ingérences malvenues. Si nous voulons avoir quelque chose d'intéressant à dire en public, il nous faut préserver la liberté d'élaborer de nouvelles idées dans la sphère privée, seuls ou avec des personnes de confiance. Il est nécessaire, pour notre liberté d'expression, que nous disposions d'un degré satisfaisant de vie privée intellectuelle, lequel se trouve menacé par la diffusion à tout-va des preuves électroniques de nos activités intellectuelles. »*

Dans son ouvrage « *Intellectual Privacy* » (« vie privée intellectuelle »)[221], Neil Richards estime que pour jouir effectivement du droit à la liberté d'expression, il est nécessaire de disposer d'un espace pour explorer et formuler des idées sans ingérence extérieure. En l'absence d'un tel espace, la protection de la liberté d'expression risque d'être vidée de son sens, car il deviendrait impossible d'élaborer des idées valant la peine d'être protégées. Ce raisonnement s'applique aussi à l'utilisation de la télévision au domicile. L'espace évoqué par Neil Richards comprend des emplacements physiques (« vie privée spatiale[222] ») ainsi que des « espaces intellectuels[223] », également évoqués en termes de « liberté d'exploration intellectuelle privée ». Avec les principes fondamentaux de « liberté de pensée et de croyance » et de « liberté de tenir des communications confidentielles[224] », ces notions forment les éléments de base de la « vie privée intellectuelle ».

---

[220] Cohen J. E., « A Right to Read Anonymously: A Closer Look at "Copyright Management" In Cyberspace », *Connecticut Law* Review, 28, 1996, p. 2, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=17990.

[221] Richards N., « Intellectual Privacy », *Texas Law Review*, 87, 2008, p. 387,

http://ukcatalogue.oup.com/product/9780199946143.do. Voir également Richards N., *Intellectual Privacy*, 2015, *op. cit.*, note de bas de page 9.

[222] *Ibid.*

[223] *Ibid.*

[224] *Ibid.*

La Cour européenne des droits de l'homme a adopté une démarche similaire dans sa jurisprudence et exprimé des inquiétudes qui font écho à celles qu'évoque Neil Richards. Elle relève ainsi que « les pensées et opinions relatives à des enjeux publics sont d'une nature vulnérable » et ajoute :

> *« En conséquence, la possibilité même d'une ingérence par les autorités **ou par des acteurs privés en l'absence d'un contrôle suffisant**, voire avec l'appui des autorités, **peut peser lourdement sur la libre formation des idées** ainsi que sur le débat démocratique et avoir un effet dissuasif*[225]*. »* (soulignement ajouté)

L'effet dissuasif sur la liberté d'expression envisagé ici concerne le droit de chercher ou de consulter des informations et des idées sans ingérence extérieure. Il provient pour sa plus grande part de la « multiveillance » de la consommation par les utilisateurs de contenus radiodiffusés, ainsi que des autres activités en ligne qu'ils mènent grâce à leurs smart TVs (voir l'introduction pour de plus amples précisions).

4.3.2. Qu'est-ce qu'une protection adaptée ?

Après avoir défini l'objet à protéger et les raisons de sa protection, nous pouvons nous interroger sur la façon la plus adaptée de protéger cet espace. La notion de données à caractère personnel se prête particulièrement bien à la mise en œuvre de cette protection. L'opinion de Charles Fried sur le respect de la vie privée est éclairante à cet égard : « La vie privée est le contrôle que nous exerçons sur les informations qui nous concernent[226]. » Plus célèbre encore est peut-être la définition qu'en donne Alan F. Westin : « L'exigence d'individus, de groupes ou d'institutions de déterminer quand, comment et dans quelle mesure les informations les concernant sont communiquées à autrui[227]. »

Ces affirmations ont en commun deux éléments : 1) le contrôle de l'information ; et 2) les informations qui nous concernent. Le second élément n'a rien de surprenant, puisqu'il apparaît dans la définition des données à caractère personnel donnée dans le chapitre II. Ainsi que nous l'avons vu avec les articles 7 et 8 de la charte, ces droits sont étroitement liés. La protection de la vie privée ne peut exister sans le contrôle exercé par l'individu sur ses données à caractère personnel.

Le concept-clé permettant d'évaluer le degré d'adéquation de la protection est le *contrôle*. Cette notion renvoie à l'autonomie des individus pour contrecarrer les ingérences dans leur vie privée. Ou, comme l'exprime Beate Rössler :

> *« Si certaines personnes appréhendent ces formes de violation de la vie privée informationnelle comme une déprédation ou une aliénation, ce n'est pas seulement parce qu'elles les perçoivent comme des désagréments, des humiliations ou des offenses et les rejettent pour cette raison, même si ce point y joue un rôle. Cela tient aussi et surtout au fait que ces violations de la vie privée informationnelle s'accompagnent toujours d'atteintes aux conditions de l'autonomie. L'autonomie de l'individu est conditionnée par sa vie privée informationnelle*[228]*. »*

---

[225] Arrêt de la Cour européenne des droits de l'homme, affaire *Altuğ Taner Akçam c. Turquie*, requête n° 27520/07, 25 octobre 2011, par. 81, http://hudoc.echr.coe.int/eng?i=001-107206#{"itemid" : ["001-107206"]}.

[226] Fried C., « Privacy », *Yale Law Journal*, 77, 1968, p. 482.

[227] Westin A. F., *Privacy and Freedom* », New York: Atheneum 1967, p. 7.

[228] Rössler B., *Der Wert des Privaten*, Suhrkamp, Francfort-sur-le-Main, 2001, p. 203, http://www.suhrkamp.de/buecher/der_wert_des_privaten-beate_roessler_29130.html.

La nécessité de contrôler ces informations joue un rôle central dans la position des organismes de surveillance allemands et néerlandais compétents pour le respect de la vie privée en ce qui concerne le degré de protection requis pour les smart TVs. Comme indiqué dans son enquête sur TP Vision[229], l'Autorité néerlandaise de protection des données a dressé la liste des exigences garantissant le respect de la législation relative à la protection des données. Cela ne démontre pas nécessairement le caractère adéquat de cette législation, mais illustre l'importance donnée aux moyens d'accroître l'autonomie de l'individu. Parmi ces exigences figure une description précise des finalités du traitement de données qui doit permettre à la personne d'accorder son consentement éclairé. Les devoirs d'information jouent donc un rôle important dans les opinions de l'Autorité néerlandaise de protection des données. Les quatre règles générales susmentionnées qu'il convient de respecter en ce qui concerne les smart TVs, telles qu'énoncées par les autorités allemandes compétentes, doivent également être prises en compte[230] :

On notera que la position des autorités allemandes prévoit notamment la possibilité d'utiliser le téléviseur de façon anonyme, une réflexion qui rejoint le « droit de lire anonymement » de Julie Cohen évoqué au début de cette partie.

En conséquence, les principes qui suivent pourraient former un point de départ en vue de déterminer ce qui constitue une protection adéquate. Celle-ci suppose d'abord qu'il soit possible d'utiliser une smart TV de façon complètement anonyme. C'est seulement à cette condition que l'utilisateur pourra effectivement bénéficier de l'espace sécurisé dont il a besoin pour sa « vie privée intellectuelle ». Pour ce faire, il est nécessaire que toutes les informations utilisées pour le traitement des données à caractère personnel lui soient présentées clairement et par ordre décroissant d'incidence. En outre, pour une protection adaptée, le traitement doit reposer sur le consentement de l'utilisateur, afin que celui-ci puisse exercer un contrôle effectif sur ses données à caractère personnel. Le traitement ne doit d'ailleurs être possible que sur la base de cette condition. Si le refus de l'utilisateur le prive de certains services, il convient d'évaluer si cette conséquence est raisonnable. Il est par exemple difficile d'établir des suggestions de contenus sans profil d'utilisateur, mais si l'utilisateur objecte à la création d'un profil, il pourrait se voir refuser l'accès au service. De nombreux utilisateurs considéreraient qu'il s'agit là d'une solution raisonnable, dès lors qu'ils disposent d'une information claire en amont.

L'instauration d'un degré de protection adapté requiert aussi l'application par le fournisseur de smart TVs des principes de « respect de la vie privée dès la conception » et/ou de « respect de la vie privée par défaut ». Les utilisateurs peu versés dans la technologie pourraient ainsi effectuer un choix éclairé avant de se servir de l'appareil.

Le degré de contrôle conféré aux utilisateurs devrait s'appliquer à l'intégralité du « cycle de vie » du traitement : responsable du traitement, sous-traitant et sous-traitant ultérieur. Il s'ensuit que l'utilisateur doit avoir la maîtrise de la conservation ou de la suppression de ses données à caractère personnel.

4.3.3. Le règlement offre-t-il un degré de protection adapté ?

Ayant défini la notion de protection adaptée, nous pouvons à présent examiner si le règlement répond à ce critère. Pour ce faire, nous allons étudier les différentes dispositions pertinentes.

[229] Autorité néerlandaise de protection des données, *op. cit.*, note de bas de page 109.

[230] *Ibid.*, note de bas de page 73.

4.3.3.1. Anonymat

Le règlement ne mentionne le terme « anonyme » que dans le considérant 23, qui exclut expressément les informations anonymes de la notion de données à caractère personnel, puisque la personne concernée n'est plus identifiable[231]. La notion d'anonymat n'est pas abordée ailleurs, puisqu'elle ne figure pas parmi les objectifs du règlement, lequel se concentre sur les principes et les conditions du traitement. Cette approche part du principe et accepte que le traitement des données à caractère personnel a lieu ; l'objectif et de mettre en place des garanties pour cette pratique. Peut-être est-il toutefois possible d'interpréter l'exigence de consentement comme une forme d'anonymat.

4.3.3.2. Consentement

Ainsi que nous l'avons vu plus haut, le traitement licite des données à caractère personnel n'est possible que sur la base des conditions énumérées à l'article 6, parmi lesquelles figure le consentement. Comme nous l'avons souligné précédemment, le traitement de données à caractère personnel issues des smart TVs ne devrait être possible *que* moyennant le consentement des intéressé(e)s, toutes les autres conditions n'offrant qu'un contrôle insuffisant à la personne concernée. Toutefois, le règlement évoque cinq autres critères en sus du consentement, dont deux pourraient s'adapter au traitement des données des smart TVs. Le degré de protection semble inadéquat en la matière, puisqu'aucune clause n'obligerait Samsung ou tout autre fournisseur à obtenir le consentement de la personne concernée. Pour y remédier, il serait possible de créer une catégorie distincte de « services fondamentaux », soumise à un régime similaire à celui des « catégories spéciales » de données à caractère personnel dans la directive, qui ne prévoit que le consentement comme motif de traitement. Il s'agirait de services (ou d'équipements) fondamentaux qui jouent un rôle important dans le quotidien des utilisateurs et sont essentiels à la connaissance et à l'information. On peut citer ainsi la télévision, l'internet, mais aussi les médiathèques. Une initiative comparable avait déjà été entreprise lorsque l'Autorité néerlandaise de protection des données avait interdit aux radiodiffuseurs publics d'employer un « *cookie-wall*[232] » (mécanisme conditionnant l'accès à un site à l'acceptation des *cookies*). Les ramifications ultérieures d'une telle démarche seraient difficiles à prédire, mais elle répondrait au besoin de protection de la « vie privée intellectuelle ».

L'exigence de consentement fixée par le règlement comporte une définition détaillée, selon laquelle tout consentement implicite ou par défaut est exclu. Il s'agit d'une évolution bienvenue, puisqu'elle confère à la personne concernée un contrôle accru. Consentement et anonymat sont en conflit, puisqu'un refus d'autorisation doit également être enregistré comme une forme de préférence. Un débat similaire a lieu en ce qui concerne les *cookies*, dans la mesure où c'est un *cookie* qui sert à enregistrer le fait qu'un utilisateur refuse leur emploi. Cela ne doit toutefois pas être une source de préoccupation, car l'incidence de cet unique traitement est limitée. Le principe du « respect de la vie privée par défaut » pourrait également fournir une issue en faisant de l'utilisation anonyme la configuration par défaut : ce réglage de base permettrait d'atteindre un certain degré d'anonymat. Il ne s'agit toutefois pas d'une solution miracle, ainsi que l'indique Frederik Zuiderveen Borgesius dans son article « Privacybescherming online kan beter: De mythe van

[231] Document du Conseil 10391/15, *op. cit.*, note de bas de page 166.

[232] Autorité néerlandaise de protection des données, « Brief aan de staatssecretaris van Onderwijs, Cultuur en Wetenschap, inzake cookiebeleid NPO », 31 janvier 2013, https://cbpweb.nl/sites/default/files/atoms/files/med_20130205-cookies-npo.pdf.

geïnformeerde toestemming[233] » (« La protection de la vie privée en ligne peut être améliorée : le mythe du consentement éclairé »). Son raisonnement repose sur l'observation selon laquelle nombre de personnes ont tendance à cliquer sur « oui » dès que c'est nécessaire, de sorte que la protection accordée par les lois relatives à la protection des données est pour l'essentiel illusoire. L'auteur suggère de mettre l'accent sur l'*autonomisation* de l'utilisateur (une notion comparable au principe de contrôle présenté auparavant) et sur la *protection.* Cette dernière doit être mise en place par la législation. Ainsi que nous l'avons vu, le législateur de l'Union s'est efforcé d'améliorer les exigences de consentement dans le règlement. Selon nous, les faiblesses relatives à cette exigence ont été corrigées de façon adéquate par le règlement, qui offre aux personnes concernées un degré de contrôle suffisant. Une possibilité d'amélioration consisterait à rendre l'exigence de consentement obligatoire pour les services et équipements fondamentaux.

Il convient de souligner que certains services, tels que Facebook, deviennent inaccessibles si l'utilisateur ne consent pas au traitement de ses données. Actuellement, la seule solution est donc de ne pas les utiliser. Toutefois, ce choix se trouve compliqué par les effets de réseau importants de bon nombre de services en ligne. Chacun peut choisir un service qui n'enfreint pas systématique ses droits, mais il est peu probable que ses amis y soient également inscrits. L'exigence actuelle de consentement n'y change rien. L'accès aux services n'est pas gratuit : les utilisateurs doivent fournir leurs données à caractère personnel au lieu de payer en numéraire. Une solution consisterait à proposer une option payante ou à offrir une version minimale du service ne comportant que les fonctionnalités de base. A cet égard, l'article 7, paragraphe 4, du règlement est important, puisqu'il interdit que l'exécution d'un contrat ou la fourniture d'un service soit soumise à la condition préalable du consentement au traitement de données qui ne sont pas nécessaires à l'exécution du contrat ou à la fourniture du service[234].

4.3.3.3. Autres exigences

Les autres exigences permettant d'obtenir un degré de protection adéquat, telles que le « respect de la vie privée dès la conception », le contrôle de l'effacement des données à caractère personnel et le devoir d'information claire, figurent dans le règlement. Comme l'a montré l'analyse qui précède, les responsables du traitement et les sous-traitants doivent veiller à la protection des données « dès la conception » en vertu de l'article 23. En outre, le « droit à l'oubli », le devoir d'information et le retrait du consentement sont également présents dans le texte. Des garanties supplémentaires telles que le « droit d'opposition », ainsi que les règles sur le profilage et les transferts internationaux de données renforcent encore le cadre général et, partant, le degré de protection des personnes concernées.

Nous pouvons en conclure que le règlement s'approche d'un degré de protection adéquat. Si les fournisseurs de smart TVs et les tierces parties telles que Netflix respectent ses prescriptions, les utilisateurs de smart TVs seront en mesure d'exercer un contrôle effectif sur leurs données à caractère personnel. L'exigence de consentement est d'une importance centrale et devrait être obligatoire selon cette hypothèse. Sur ce point, le règlement pourrait encore être amélioré. Ce n'est qu'en insistant sur cette condition qu'il sera possible de garantir aux utilisateurs la possibilité de visionner des contenus de façon anonyme.

---

[233] Zuiderveen Borgesius F., « Privacybescherming online kan beter – De mythe van geïnformeerde toestemming », *Nederlands juristenblad*, 2015-14, n° 680, p. 878-883, http://www.ivir.nl/publicaties/download/1536.

[234] *Ibid.* note de bas de page 205.

Analyse finale

Les « *big data* » ou mégadonnées ont indéniablement fait leur entrée dans le secteur audiovisuel. Les services non linéaires complètent et – surtout – supplantent rapidement la radiodiffusion traditionnelle, mais les premiers comme la seconde ont cessé d'être « déconnectés » de l'utilisateur. L'interconnectabilité permet aux fournisseurs et aux utilisateurs d'interagir. Grâce aux échanges de données à caractère personnel, qui constituent une nouvelle monnaie, les fournisseurs peuvent optimiser leur offre, tandis que les utilisateurs se voient proposer des recommandations et des sélections à partir de leur profil personnel. La médaille a toutefois son revers : inquiétudes de manipulation, concentration sur les services les plus rentables, réduction du choix pour le consommateur et manque d'information.

Les smart TVs offrent l'un des exemples les plus limpides de ces évolutions. Connectés à internet, ils offrent toutes les possibilités évoquées ci-dessus et leur généralisation ne pourra plus être enrayée. D'ici à un ou deux ans, la majorité des foyers européens en possédera un. Si l'on tient compte en outre des autres appareils présentant des fonctionnalités similaires (tablettes, smartphones et récepteurs numériques), le point de non-retour est déjà atteint.

Dans le présent *IRIS Spécial*, nous avons décrit dans le détail les fonctionnalités des smart TVs et examiné les principaux aspects du cadre réglementaire et des axes stratégiques retenus. Nous avons également retracé le contexte des premières affaires judiciaires au cours desquelles des inquiétudes concernant l'incidence de ces téléviseurs sur le respect de la vie privée ont été exprimées. Il est possible d'en tirer au moins les conclusions qui suivent.

1. Les smart TVs posent des questions de nature multiple eu égard au respect de la vie privée, car leur écosystème regroupe de nombreux fournisseurs qui mènent des activités de traitement diverses portant sur les données à caractère personnel des utilisateurs. Ces informations sont collectées via des interactions traditionnelles (télécommandes, par exemple) et/ou grâce à des plateformes proposant des sélections (c'est-à-dire des guides électroniques de programmes). Les téléviseurs sont toutefois plus « intelligents » encore : ils disposent de fonctions de reconnaissance vocale et faciale, mais aussi de commande gestuelle, et collectent et utilisent les données de l'utilisateur dans le cadre de son compte personnel. La liste n'est pas exhaustive et on peut partir du principe que le progrès technologique lui adjoindra de nouvelles options. Grâce aux applications, il est possible de combiner données physiques et médicales avec l'utilisation de contenus audiovisuels.
2. L'analyse du contexte juridique et des orientations politiques retenues révèle une situation morcelée, composée d'une réglementation spécifiquement applicable aux médias (Directive SMAV, par exemple), d'autres textes sectoriels (relatifs aux télécommunications, au commerce électronique ou au respect de la vie privée) et de règlements généraux sur la confidentialité des données applicables aux smart TVs (la directive sur la protection des données et le RGPD). Un cadre général de droits fondamentaux vient compléter ce tableau, portant au premier chef sur la liberté d'expression et la protection de la vie privée et des données.

3. La réglementation des médias traditionnels (Directive SMAV, par exemple) repose sur une longue tradition remontant aux années 1970. A l'époque, le législateur n'avait pas jugé utile d'aborder les questions d'interactivité ou de respect de la vie privée. Même les dernières révisions de ces textes visaient essentiellement à intégrer les nouvelles évolutions du point de vue de cette perspective traditionnelle : les services non linéaires ont été ajoutés au champ d'application de la réglementation, mais seulement en leur qualité de services fournissant des contenus audiovisuels sous une forme différente. Toutefois, les acteurs-clés – tant les fournisseurs de services audiovisuels que les utilisateurs – se trouvent au cœur de ce cadre traditionnel. Les possibilités et les limitations, telles que les règles relatives à la protection de la jeunesse, ont donc une incidence directe sur les potentialités de l'écosystème de la télévision intelligente.
4. Les fonctionnalités et la praticabilité de la télévision intelligente sont influencées plus directement encore par d'autres instruments sectoriels plus généraux, qui ne visent pas spécifiquement le domaine de l'audiovisuel. Tel est le cas de la réglementation sur les communications, qui a une incidence sur les infrastructures sous-jacentes (internet, par exemple) et offre des garanties pour les échanges d'informations. Les directives de l'Union européenne consacrées au secteur des communications accordent une attention particulière à l'accès conditionnel, aux guides électroniques de programmes et aux interfaces. Etant donné que ces mécanismes sont de plus en plus liés au choix des consommateurs et à la possibilité de trouver les contenus, leur importance ira en augmentant. Les aspects transactionnels de la télévision intelligente complexifient la conception traditionnelle de la compétence juridique : si celle-ci est avant tout liée au pays d'origine du service dans le secteur de l'audiovisuel, les consommateurs peuvent faire valoir leurs droits dans leur propre pays en droit de la consommation.
5. Les questions que soulèvent les nouvelles évolutions telles que les smart TVs illustrent l'importance des instruments génériques qui s'y appliquent. Le règlement général sur la protection des données a une incidence directe sur la collecte, le traitement et la conservation des données à caractère personnel recueillies grâce aux smart TVs. Pour définir le champ d'application de la législation relative à la protection des données, ce ne sont pas les définitions des catégories de services soumis à la réglementation qui comptent, mais le simple fait qu'un traitement de données à caractère personnel ait lieu et l'identité du sous-traitant soumis à la réglementation. Dans le même temps, le droit relatif à la protection des données ne tient nullement compte des fonctions et du rôle particuliers des services de médias audiovisuels pour la société et la démocratie. Il n'accorde pas non plus de protection spécifique aux utilisateurs de services de médias audiovisuels via leurs smart TVs.
6. Les droits fondamentaux pèsent également sur l'évolution de l'environnement réglementaire et des politiques. Ils fournissent aux Etats des orientations quant à la manière de garantir une protection effective des droits de l'individu à la liberté d'expression, à la vie privée et à la protection des données. Cette protection passe nécessairement par une série d'obligations positives et négatives pour les Etats. Les obligations positives pourraient avoir des répercussions sur les activités de tous les types d'acteurs de l'écosystème de la télévision numérique, dès lors que ces activités empiètent sur les droits fondamentaux.
7. A brève échéance, les smart TVs – comme *totum pro parte* – poseront des défis de taille, non seulement pour les services, avec des retombées sur le secteur et sur les utilisateurs, mais aussi du point de vue de la réglementation et des orientations stratégiques. Le paysage réglementaire dispersé doit être évalué selon une perspective plus intégrée, ce qui contribuera à déterminer si tous les aspects pertinents sont pris en compte de façon cohérente. Cette analyse révélera peut-être que certains instruments

sont dépassés et peuvent être abrogés ou modifiés. Puisque les smart TVs nous montrent à quelle vitesse la situation est susceptible d'évoluer, une démarche normative pourrait être nécessaire, car des règles gravées dans le marbre ne permettent pas de suivre la dynamique du secteur. Les instruments généraux fournissent généralement une approche plus normative, mais requièrent souvent davantage d'efforts au stade de l'application et de l'exécution. C'est une source de défis pour le régulateur : les autorités chargées des médias, du respect de la vie privée et du droit des consommateurs doivent travailler main dans la main et coordonner leurs actions. Cette coordination semble l'approche la plus vraisemblable à plusieurs égards : la construction d'un cadre stratégique et réglementaire tenant compte de tous les aspects, trop utopique et trop chronophage, ne correspondrait en outre ni aux intérêts des fournisseurs de services ni à ceux des utilisateurs.

OBSERVATOIRE EUROPÉEN DE L'AUDIOVISUEL

Institué en décembre 1992, l'Observatoire européen de l'audiovisuel a pour objectif de collecter et de diffuser des informations sur l'industrie audiovisuelle en Europe.
L'Observatoire est un organisme de service public européen, composé de 41 Etats membres et de l'Union Européenne, représentée par la Commission Européenne. Il exerce son activité dans le cadre juridique du Conseil de l'Europe et travaille en collaboration avec un certain nombre d'organismes professionnels et partenaires du secteur audiovisuel, ainsi qu'avec un réseau de correspondants.

Les principales activités de l'Observatoire européen de l'audiovisuel portent sur :

- l'Annuaire service en ligne
  www.yearbook.obs.coe.int
- la publication de rapports et de bulletins d'information
  www.obs.coe.int/publications
- la mise à disposition d'informations grâce à son site Internet
  www.obs.coe.int
- des contributions aux conférences
  www.obs.coe.int/events

L'Observatoire met également à disposition, gratuitement, des bases de données :

IRIS Merlin
Base de données sur les informations juridiques relatives au secteur audiovisuel en Europe
www.merlin.obs.coe.int

MAVISE
Base de données sur les chaînes TV, les services audiovisuels à la demande et les entreprises en Europe
www.mavise.obs.coe.int

AVMSDatabase
Base de données sur la transposition de la Directive SMAV dans la législation nationale
www.avmsd.obs.coe.int

LUMIERE
Base de données sur les entrées des films distribués en Europe
www.lumiere.obs.coe.int

Observatoire européen de l'audiovisuel
76 Allée de la Robertsau – 67000 Strasbourg – France
Tél.: +33 (0) 3 90 21 60 00 – Fax: +33 (0) 3 90 21 60 19
www.obs.coe.int – E-mail: info.obs@coe.int

IRIS Spécial

Smart TV et protection des données

Samsung a averti les personnes possédant un smart TV de la marque que la reconnaissance vocale du système peut enregistrer et partager leurs conversations privées. Ce « mauvais buzz » survient alors que Bruxelles est sur le point d'adopter un nouveau texte de loi – le règlement général sur la protection des données (RGPD) – visant à nous protéger contre les usages abusifs de nos données privées et autres « big data » concernant notre comportement de consommation collectées par des appareils intelligents tels que les téléviseurs. L'Observatoire européen de l'audiovisuel, qui fait partie du Conseil de l'Europe à Strasbourg, suit ces évolutions et a publié ce rapport IRIS *Spécial* intitulé « Smart TV et protection des données ».

Il s'agit d'une publication conjointe de l'Observatoire basé à Strasbourg et de son organisation partenaire, l'Institut néerlandais du droit de l'information (IViR, basé à Amsterdam). Il a inspiré un atelier d'experts organisé à Strasbourg en décembre 2015 sur le thème « les zones d'ombre entre régulation des médias et protection des données ».

OBSERVATOIRE EUROPÉEN DE L'AUDIOVISUEL

EUR 49 - 978-92-871-8238-8