Université de Lausanne
Faculté de droit, des sciences criminelles et d'administration publique

MÉMOIRE DE MASTER

RÉSEAUX SOCIAUX ET CIBLAGE PUBLICITAIRE: PROCESSUS ET FONDEMENT JURIDIQUE DU TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL

Présenté par

Djamila-Jane Limat

Sous la direction du Professeur Sylvain Métille

Lausanne, le 26 avril 2019

* * *

Bibliographie

ANDREOU ATHANASOS/VENKATADRI GIRIDHARI/GOGA OANA/GUMMADI KRISHNA P./LOISEAU PATRICK/MISLOVE ALAN, *Investigating Ad Transparency Mechanisms in Social Media: A Case Study of Facebook's Explanations,* in: Network and Distributed Systems Security (NDSS) Symposium 2018, San Diego 2018 (cité ANDREOU ET AL.). Disponible sur: https://www.ndss-symposium.org/wp-content/uploads/2018/02/ndss2018_10-1_Andreou_paper.pdf.

ANTREASYAN SEVAN, *Réseaux sociaux et mondes virtuels - Contrat d'utilisation et aspects de propriété intellectuelle*, thèse, Université de Genève, Genève 2016 (cité ANTREASYAN).

AUF DER MAUR ROLF/FEHR-BOSSHARD DELIA, *Personalisierte Werbung,* in: Center for Information Technology Society and Law (ITSL), Volume 1, Zurich/Bâle/Genève 2017, pp. 23-60 (cité AUF DER MAUR/FEHR-BOSSHARD).

BAERISWYL BRUNO, *Entwicklungen im Datenschutzrecht - Le point sur le droit de la protection des données*, RSJ 114/2018, pp. 450-452 (cité BAERISWYL, *Datenschutzrecht*).

BAERISWYL BRUNO, *Die Anwendbarkeit des Datenschutzgesetzes Schweizerisches Datenschutzrecht ist auch auf den Internetdienst "Street View" anwendbar*, in: digma - Zeitschrift für Datenrecht und Informationssicherheit, 2009, pp. 98-101 (cité BAERISWYL, *« Street View »*).

BAERISWYL BRUNO/PÄRLI KURT (édit.), *Handkommentar Datenschutzgesetz,* Berne 2015 (cité Auteur, in: HK DSG).

BEELEN AXEL, *Guide pratique du RGPD - Fiches de guidance,* Bruxelles 2018 (cité BEELEN).

BÖPPLE OLIVER/GLENDE SEBASTIAN/SCHAUBER CORNELIA, *Innovative Einkaufserlebnisse mit Beacon-Technologie gestalten,* in: Marktplätze im Umbruch: digitale Strategien für Services im Mobilen Internet, Berlin 2015, pp. 299-307 (cité BÖPPLE/GLENDE/SCHAUBER).

BOUMANS WILLEM, *Web Tracking And Current Countermeasures*, thèse, Université de Radboud, Nimègue 2017 (cité BOUMANS).

BUCHNER BENEDIKT, *Die Einwilligung im Datenschutzrecht - vom Rechtfertigungsgrund zum Kommerzialisierungsinstrument,* in: Datenschutz und Datensicherheit - DuD, Volume 34, Issue 1, 2010, pp. 39-43 (cité BUCHNER).

BYGRAVE LEE A., *Minding the machine: Article 15 of the EC Data Protection Directive and Automated Profiling*, in: Computer Law & Security Report - CLSR, Volume 17, Issue 1, janvier, 2001, pp. 17-24 (cité BYGRAVE).

CATANESE SALVATORE A./DE MEO PASQUALE/FERRARA EMILIO/FIUMARA GIACOMO/PROVETTIA ALESSANDRO, *Crawling Facebook for Social Network Analysis Purposes,* in: WIMS'11 Proceeding of the International Conference on Web Intelligence, Mining and Semantics, Sogndal 2011 (cité CATANESE ET AL.). Disponible sur https://dl.acm.org/citation.cfm?doid=1988688.1988749.

CELLINA EVA, *L'administrateur d'une page fan Facebook - co-responsable du traitement - Commentaire de l'arrêt de la CJUE (Grande Chambre) C-210/16 du 5 juin 2018,* in: Jusletter 10 septembre 2018 (cité CELLINA).

CHARLET FRANÇOIS, *Réseaux sociaux et protection des données - Analyse des pratiques de Facebook en regard des exigences des droits européen et suisse de la protection des données,* in: A. Epiney/D. Sangsue (édit.), *Digitalisierung und Schutz der Privatsphäre/L'ère numérique et la protection de la sphère privée - Zur Steuerungsfähigkeit der « traditionellen » Rechtsgrundsätze: Analyse und Perspektiven/L'impact des principes juridiques « traditionnels »: analyse et perspectives*, Zurich/Bâle/Genève 2018, pp. 77-115 (cité CHARLET).

COMITÉ CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT AUTOMATISÉ DE DONNÉES À CARACTÈRE PERSONNEL, *L'application de la Convention 108 au mécanisme de profilage - Eléments de réflexion destinés au travail du futur Comité consultatif (T-PD)*, Strasbourg 2008 (cité COMITÉ CONSULTATIF).

COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES (CEPD), *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*, adoptées le 9 avril 2019 (cité CEPD).

COMMISSION NATIONALE DE L'INFORMATIQUE & DES LIBERTÉS, *communication du 5 février 2009 concernant la publicité ciblée en ligne* (cité CNIL).

CAVOUKIAN ANN, *Data Mining: Staking a Claim on Your Privacy*, Information and Privacy Commissioner, Ontario 1998 (cité CAVOUKIAN).

DE TERWANGNE CÉCILE ET AL., *Le Règlement général sur la protection des données (RGPD/GDPR): analyse approfondie*, Bruxelles 2018 (cité Auteur, in: *Le Règlement général sur la protection des données*).

EBERSOHN GERRIE, *Internet Law: Cookies, Traffic Data and Direct Advertising Practices,* in: SA Mercantile Law Journal - SAMLJ, Volume 16, Issue 4, janvier, 2004, pp. 741-764 (cité EBERSOHN).

ESTEVE ASUNCION, *The business of personal data: Google, Facebook, and privacy issues in the EU and the USA,* in: International Data Privacy Law - IDPL, Volume 7, Issue 1, février, 2017, pp. 36-47 (cité Esteve).

GOLA PETER, *Datenshutz-Grundverordnung VO (EU) 2016/679, Kommentar,* Munich 2017 (cité Auteur, in: Kommentar DS-GVO).

GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES, *Avis 4/2007 sur le concept de données à caractère personnel - WP136*, 20 juin 2007 (cité GR29, WP136).

GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES, *Avis 5/2009 sur les réseaux sociaux en ligne - WP163*, 12 juin 2009 (cité GR29, WP163).

GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES, *Avis 2/2010 sur la publicité comportementale en ligne - WP171,* 22 juin 2010 (cité GR29, WP171).

GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES, *Avis 15/2011 sur la définition du consentement - WP187,* 13 juillet 2011 (cité GR29, WP187).

GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES, *Avis 04/2012 sur l'exemption de l'obligation de consentement pour certains cookies - WP194*, 7 juin 2012 (cité GR29, WP194).

GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES, *Avis 03/2013 sur la limitation des finalités - WP203,* 2 avril 2013 (cité GR29, WP203).

GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES, *Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage aux fins du règlement (UE) 2016/679 - WP251 rév.01,* révisées et adoptées le 6 février 2018 (cité GR29, WP251 rév.01).

GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES, *Lignes directrices sur le consentement au sens du règlement 2016/679 - WP259 rév.01*, révisées et adoptées le 10 avril 2018 (cité GR29, WP259 rév.01).

HADMI AZHAR, *Protection des données visuelles - Analyse des fonctions de hachage perceptuel*, thèse, Université de Montpellier, Montpellier 2012 (cité HADMI).

HILDEBRANDT MIREILLE, *Who is Profiling Who ? Invisible Visibility,* in: S. Gutwirth/Y. Poullet/P. de Hert/C. De Terwangne/S. Nouwt (édit.), *Reinventing Data Protection*, Dordrecht 2009, pp. 239-252 (cité HILDEBRANDT, *Who is Profiling Who*).

HILDEBRANDT MIREILLE, *Defining Profiling: A New Type of Knowledge ?,* in: M. Hildebrandt/S. Gutwirth (édit.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Dordrecht 2008, pp. 17-45 (cité HILDEBRANDT, *Defining Profiling*).

HOOFNAGLE CHRIS JAY/SOLTANI ASHKAN/GOOD NATHAN/WAMBACH DIETRICH JAMES/AYENSON MIKA D., *Behavioral Advertising: The Offer You Cannot Refuse,* in: Harvard Law & Policy Review, Volume 6, Issue 2, août, 2012, pp. 273-296 (cité HOOFNAGLE ET AL.).

JAHNEL DIETMAR/BERGAUER CHRISTIAN, *Teil-Kommentar zur DS-GVO - Datenschutz-Grundverordnung - Kommentar zu den Art 2-4, 13-44, 30, 35, 37-37,* Vienne 2018 (cité JAHNEL/BERGAUER, in TK DS-GVO).

JOLER VLADAN/PETROVSKI ANDREJ, *Immaterial Labour and Data Harvesting - Facebook Algorithmic Factory (1),* in: SHARE LAB 2016 (cité JOLER/PETROVSKI, *Immaterial Labour*, disponible sur: https://labs.rs/en/facebook-algorithmic-factory-immaterial-labour-and-data-harvesting/).

JOLER VLADAN/PETROVSKI ANDREJ, *Quantified Lives on Discount - Facebook Algorithmic Factory (3),* in: SHARE LAB 2016 (cité JOLER/PETROVSKI, *Quantified Lives,* disponible sur: https://labs.rs/en/quantified-lives/).

JOUX ALEXANDRE, *Publicité ciblée et régies en ligne: quand le marché se structure*, in: La revue européenne des médias et du numérique, n°6-7, 2008, pp. 48-58 (cité JOUX).

KARG MORITZ/THOMSEN SVEN, *Tracking und Analyse durch Facebook - Das Ende der Unschuld,* in: Datenschutz und Datensicherheint - DuD, Volume 36, Issue 10, 2012, pp. 729-736 (cité KARG/THOMSEN).

KELSHAW TOM, *Analyser les émotions pour optimiser l'efficacité publicitaire*, août 2017 (cité KELSHAW, *Analyser les émotions,* disponible sur: https://www.thinkwithgoogle.com/intl/fr-145/industry-perspectives/articles-internationaux/analyse-de-lemotion-une-solution-efficace-pour-ameliorer-lintuition/).

KETTIGER DANIEL, *Rechtliche Rahmenbedingungen für Location Sharing Systems in der Schweiz,* in: Jusletter 9 août 2010 (cité KETTIGER).

KING NANCY J./FORDER JAY, *Data analytics and consumer profiling: Finding appropriate privacy principles for discovered data,* in: Computer Law and Security Review - CLSR, Volume 32, Issue 5, octobre, 2016, pp. 696-714 (cité KING/FORDER).

KIRSCH MATTHEW S., *Do Not Track: Revising the EU's Data Protection Framework to Require Meaningful Consent for Behavioral Advertising*, in: Richmond Journal of Law and Technology - JOLT, Volume 18, Issue 1, pp. 1-50 (cité KIRSCH).

KÜHLING JÜRGEN/BUCHNER BENEDIKT, *Datenschutz-Grundverordnung/BDSG, Kommentar,* 2e éd., Munich 2018 (cité Auteur, in: DS-GVO Kommentar).

LEONARD THIERRY, *E-marketing et protection des données à caractère personnel,* Bruxelles 2000 (cité LEONARD).

LEROY FRANCK, *Réseaux sociaux & Cie - Le commerce des données personnelles,* Arles 2013 (cité LEROY).

MATHYS ROLAND/MEIER CHRISTIAN, *Tracking - rechtliche Standortbestimmung,* in: digma - Zeitschrift für Datenrecht und Informationssicherheit, 2014, pp. 156-160 (cité MATHYS/MEIER).

MAURER-LAMBROU URS/BLECHTA GABOR P. (édit.), *Basler Kommentar, Datenschutzgesetz - Öffenlichtkeitsgesetz,* 3e éd., Bâle 2014 (cité Auteur, in: BSK DSG/BGO).

MAYER JONATHAN R./MITCHELL JOHN C., *Third-Party Web Tracking: Policy and Technology*, in: SP'12 Proceeding of the 2012 IEEE Symposium on Security and Privacy, Oakland 2012, pp. 413-427. Disponible sur: https://dl.acm.org/citation.cfm?id=2310703 (cité MAYER/MITCHELL).

MEIER PHILIPPE, *Protection des données - Fondements, principes généraux et droit privé*, Berne 2011 (cité MEIER).

MERCANTI-GUÉRIN MARIA/VINCENT MICHÈLE, *Publicité digitale,* Malakoff 2016 (cité MERCANTI-GUÉRIN/VINCENT).

MÉTILLE SYLVAIN, *Internet et droit - Protection de la personnalité et questions pratiques,* Genève 2017 (cité MÉTILLE).

MOHIT KUMAR, *Hundreds of Apps Using Ultrasonic Signals to Silently Track Smartphone Users,* mai, 2017 (cité MOHIT, *Hundreds of Apps Using Ultrasonic Signals,* disponible sur: https://thehackernews.com/2017/05/ultrasonic-tracking-signals-apps.html).

MORITZ MARCEL, *Les nouveaux concepts de protection de la vie privée et leur portée,* in: A. Epiney/T. Fasnacht/G. Blaser (édit.), *Instrumente zur Umsetzung des Rechts auf informationelle Selbstbestimmung /Instruments de mise en œuvre du droit à l'autodétermination informationnelle*, Zurich/Bâle/Genève 2013, pp. 47-65 (cité MORITZ).

OBERLIN JUTTA SONJA, *Social Media-Nutzung, Marketing und die DS-GVO: Wie sollten Unternehmen mit den neuen Medien und Marketingtechnologien umgehen ? - Teil 1,* in: Compliance Berater 1-2/2019, pp. 15-19 (cité OBERLIN, *Teil 1*).

OBERLIN JUTTA SONJA, *Social Media-Nutzung, Marketing und die DS-GVO: Wie sollten Unternehmen mit den neuen Medien und Marketingtechnologien umgehen ? - Teil 2,* in: Compliance Berater 3/2019, pp. 67-70 (cité OBERLIN, *Teil 2*).

PASSADELIS NICOLAS/ROSENTHAL DAVID/THÜR HANSPETER, *Datenschutzrecht - Beraten in Privatwirtschaft und öffentlicher Verwaltung,* Bâle 2015 (cité PASSADELIS/ROSENTHAL/THÜR).

PRAZ EMILIE M., *La protection des données et les réseaux sociaux,* in: Jusletter 12 janvier 2015 (cité PRAZ).

PRÉPOSÉ FÉDÉRAL A LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE (PFPDT), *Explications concernant le webtracking*, août 2013 (cité PFPDT: *Explications concernant le webtracking*, disponible sur: https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/Internet_und_Computer/webtracking/explications-concernant-le-webtracking.html)

ROGOSCH PATRICIA MARIA, *LIKE-BUTTON: welches rechtliche Risiko ?,* in: digma - Zeitschrift für Datenrecht und Informationssicherheit, 2011, pp. 182-184 (cité ROGOSCH).

ROSENTHAL DAVID/JÖHRI YVONNE (édit.), *Handkommentar zum Datenschutzgesetz*, Zurich 2008 (cité HK-ROSENTHAL/JÖHRI).

SARGSYAN MANE, *Endorsements and Behavioral Advertising in Social Media under EU, Swiss and US law - Disclosure requirements, personality rights, and data protection*, in: Center for Information Technology Society and Law (ITSL), Volume 3, Zurich/Bâle/Genève 2017 (cité SARGSYAN).

SCHLEIPFER STEFAN, *Facebook-Like-Buttons - Technik, Risiken und Datenschutzfragen,* in: Datenschutz und Datensicherheit - DuD, Volume 38, Issue 5, 2014, pp. 318-324 (cité SCHLEIPFER).

SCHWEIZER ALEX, *Data Mining - ein rechtliches Minenfeld,* in: digma - Zeitschrift für Datenrecht und Informationssicherheit, 2001, pp. 108-114 (cité SCHWEIZER, *Data Mining*).

SCHWEIZER ALEX, *Customer Relationship Management, Datenshutz- und Privatrechtsverletzungen beim CRM,* Berne/Zurich 2007 (cité SCHWEIZER, *CRM*).

SÖBBING THOMAS, *Der Datenskandal bei Facebook und die rechtliche Zulässigkeit von künstlicher Intelligenz (KI) zur Beeinflussung der politischen Willensbildung (sog. Microtargeting)*, in: InTeR, Issue 4, 2018, pp. 182-188 (cité SÖBBING).

THOUVENIN FLORENT/FRÜH ALFRED/GEORGE DAMIAN, *Datenschutz und automatisierte Entscheidungen*, in: Jusletter 26 novembre 2018 (cité THOUVENIN/FRÜH/GEORGE).

TUFFERY STÉPHANE, *Data mining et statistique décisionnelle - L'intelligence des données*, 4e éd., Paris 2012 (cité TUFFERY, *L'intelligence des données*).

TUFFERY STÉPHANE, *Data mining et statistique décisionnelle - La science des données*, 5e éd., Paris 2017 (cité TUFFERY, *La science des données*).

U.S. SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION, *A review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes - Staff report for Chairman Jay Rockefeller,* décembre, 2013 (cité U. S. SENATE COMMITTEE). Disponible sur: https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf.

WAUTERS ELLEN/LIEVENS EVA/WALCKE PEGGY, *Towards a better protection of social media users: a legal perspective on the terms of use of social networking sites,* in: International Journal of Law and Information Technology, Volume 22, Issue 3, septembre, 2014, pp. 254-294 (cité WAUTERS/LIEVENS/WALCKE).

WAUTHY XAVIER, *No free lunch sur le Web 2.0! Ce que cache la gratuité apparente des réseaux sociaux numériques,* in: Regards économiques, Volume 59, mai, 2008, pp. 1-10 (cité WAUTHY).

THOUVENIN FLORENT, *Erkennbarkeit und Zweckbindung: Grundprinzipien des Datenschutzrecht auf dem Prüfstand von Big Data,* in: R. Weber H./F. Thouvenin (édit.), *Big Data und Datenschutz - Gegenseitige Herausforderungen,* Zurich/Bâle/Genève 2014, pp. 61-83 (cité THOUVENIN).

WALTER JEAN-PHILIPPE, *Le profilage des individus à l'heure du cyber espace - un défi pour le respect du droit à la protection des données,* in: A. Epiney/T. Probst/N. Gammenthaler (édit.), *Datenverknüpfung - Problematik und rechtlicher Rahmen - L'interconnexion de données - Problématique et cadre juridique,* Zurich/Bâle/Genève 2011, pp. 87-113 (cité WALTER).

ZARSKY TAL Z., « *Mine Your Own Business ! »: Making the Case for the Implications of the Data Mining or Personal Information in the Forum of the Public Opinion*, in: Yale Journal of Law & Technology, Volume 5, Issue 1, 2003, pp. 17-47 (cité ZARSKY).

ZUIDERVEEN BORGESIUS FREDERIK J., *Informed Consent: We Can Do Better to Defend Privacy*, in: IEEE Security & Privacy, Volume 13, Issue 2, mars, 2015, pp. 103-107 (cité ZUIDERVEEN BORGESIUS).

Table des abréviations

Al.	alinéa(s)
Art.	article(s)
ATF	arrêt du Tribunal fédéral suisse
CEPD	Comité européen de la protection des données
Cf.	confer
ch.	chapitre
CJUE	Cour de justice de l'union européenne
CNIL	Commission nationale de l'informatique & des libertés (France)
consid.	considérant
DS-GVO	Datenschutz-Grundverordnung (= RGPD)
DSG	Bundesgesetz vom 19. Juni 1992 über Datenschutz (= LPD ; RS. 235.1)
éd.	édition
édit.	éditeur(s)
etc.	et caetera
ibid	ibidem locution latine signifiant « même endroit »
idem	locution latine signifiant « le même »
in	dans
i.f.	*in fine* (à la fin)
JdT	Journal des Tribunaux
let.	lettre (d'un article)
LF	Loi fédérale
LPD	Loi fédérale sur la protection des données, du 19 juin 1992 (RS. 235.1)
n°	numéro
nbp	note de bas de page
p.	page
P	projet
PFPDT	Préposé fédéral à la protection des données et à la transparence
GR29	Groupe de travail « article 29 »
RGPD	Règlement (UE) 2015/679 du 27 avril 2016 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
RS.	recueil systématique fédéral
ss	et suivant(e)s
TAF	Tribunal administratif fédéral suisse
TF	Tribunal fédéral suisse

INTRODUCTION

Les techniques performantes de collecte et d'analyse de données sont sans cesse développées et améliorées. Les bases de données sont en perpétuelle évolution. Ces techniques permettent, entre autres, aux protagonistes du secteur publicitaire de constituer des profils toujours plus précis dans le but de diffuser une publicité conforme à ces profils et susceptible d'intéresser l'internaute. Des préoccupations s'agissant de la publicité ciblée et de l'opacité des mécanismes publicitaires se font entendre. Les nouvelles technologies relatives aux capacités croissantes des processus algorithmiques permettent le suivi quotidien des utilisateurs, leur ciblage toujours plus précis ainsi que la prédiction de leurs choix, leurs comportements et leurs actions. Le Conseil de l'Europe a sur ce sujet exprimé, dans un récent communiqué de presse du 13 février 2019, ses craintes quant « au risque que les citoyens ne soient pas en mesure de se faire une opinion et de prendre des décisions en toute indépendance par rapport aux systèmes automatisés, et qu'ils fassent même l'objet de manipulations dues à l'utilisation de technologies numériques avancées, en particulier les techniques de microciblage »[1].

Les réseaux sociaux, en tant qu'acteurs recourant au profilage et aux technologies de prédiction, sont visés par ces préoccupations. Ces plates-formes sociales mettent à disposition des annonceurs des services publicitaires efficaces capables de cibler les utilisateurs susceptibles d'être intéressés par les annonces. Pour assurer la fonctionnalité d'un tel ciblage, les données des utilisateurs sont collectées de part et d'autre de la toile, tant à l'interne de la plate-forme sociale qu'à l'externe. Cependant, les réseaux sociaux ont, ces derniers mois, fait l'objet de critiques de la part de la presse et des autorités. Ces derniers les accusent de violer la législation sur la protection des données, surtout en termes de transparence et de sécurité. La difficulté principale de ces acteurs réside dans le fait de recueillir un consentement libre, éclairé, spécifique et univoque de la part des utilisateurs. Le nouveau règlement sur la protection des données (ci-après: RGPD) impose des exigences particulièrement difficiles à mettre en œuvre pour les entreprises qui exploitent des quantités considérables de données et recourent aux technologies de suivi en ligne. S'agissant des publicités ciblées, les moyens pour les élaborer, tels que les cookies, les pixels et autres technologies ou moyens de traçage, ont pour conséquence d'accroître la difficulté à satisfaire les exigences de la législation sur la protection des données, en particulier celles relatives au consentement.

Ce travail a, dans une première partie, pour objectif d'éclairer le processus de la publicité personnalisée sur les réseaux sociaux. Pour ce faire, différents moyens de suivi en ligne et de collecte de données seront présentés. Le procédé du profilage et la constitution de profils seront ensuite abordés, pour finir sur les différents mécanismes de ciblage proposés aux annonceurs. La seconde partie se focalisera sur l'exigence d'un fondement juridique au traitement des données requis par le RGPD. Après un léger rappel des principes de base et pertinents en matière de publicités ciblées, différents fondements juridiques susceptibles d'entrer en ligne de compte feront, chacun séparément, l'objet d'une analyse détaillée. Nous tenterons ainsi de découvrir si une alternative au consentement est apte à légitimer le traitement des données à des fins de ciblage publicitaire. Le cas échéant, quelles principales mesures devraient être prises par les exploitants des réseaux sociaux pour pouvoir s'en prévaloir.

[1] CONSEIL DE L'EUROPE, *communiqué de presse du 13 février 2019 sur le risque que les processus algorithmiques soient utilisés pour manipuler les comportements sociaux et politiques*.

PARTIE 1: ASPECTS « TECHNIQUES » RELATIFS AU TRAITEMENT DE DONNÉES À DES FINS DE CIBLAGE PUBLICITAIRE

CHAPITRE 1: GÉNÉRALITÉS

A. Quelques définitions clés

1. Réseaux sociaux

Un réseau social se définit comme une plate-forme de communication en ligne permettant à ses utilisateurs de partager des intérêts communs et d'interagir entre eux[2]. Il est en général proposé aux membres de mettre en ligne leur propre contenu ou ceux de tiers, tel que des photos, des vidéos, des textes, des liens ou des commentaires, qui seront accessibles et visibles par d'autres utilisateurs. Les membres créent un profil ou un compte complété par des informations personnelles les concernant et dont l'accès est en principe autorisé à tout un chacun. Selon ANTREASYAN[3], un réseau social se caractérise par plusieurs critères: *la persistance*, en ce sens que l'existence d'un réseau social est continue et indépendante de l'utilisateur, *l'univers informatique* car le fonctionnement d'un réseau social repose sur un système informatique comme un logiciel ou un set d'applications et l'*interaction* entre les utilisateurs membres du réseau social favorisant ainsi les échanges et la génération de contenu.

2. Utilisateur

Il s'agit de la personne qui, après avoir accepté les conditions générales d'utilisation préétablies par l'exploitant d'un réseau social[4], devient membre de la communauté de ce réseau. L'utilisateur se trouve dans une relation contractuelle avec l'exploitant de la plate-forme et a, à ce titre, des droits et des obligations vis-à-vis de la plate-forme[5]. Il s'agit également de la personne qui, du moins en grande partie, génère et diffuse du contenu au sein de la plate-forme, y compris des informations personnelles le concernant lui ou des tiers[6]. À ce titre, l'utilisateur est à la fois « consommateur et fournisseur de contenus »[7].

---

[2] GR29, WP163, pp. 4-5. *Cf.* aussi: SARGSYAN, pp. 3-4.
[3] ANTREASYAN, pp. 7-12.
[4] SARGSYAN, p. 6.
[5] Pour davantage d'informations concernant les droits et obligations de l'utilisateur vis-à-vis de l'exploitant d'un réseau social, voir ANTREASYAN, p. 60 ss. Nous pouvons citer à titre d'exemple l'obligation de l'utilisateur d'octroyer à l'exploitant l'autorisation d'utiliser les informations personnelles qu'il fournit à la plate-forme et celles qu'il publie de façon visible au public ou aux autres utilisateurs, le contenu qu'il génère et les informations résultant d'un contenu généré et de permettre le traitement de ses données à des fins commerciales notamment. Pour en savoir davantage sur les informations recueillies et traitées, voir la politique d'utilisation des données Facebook, *Quels types d'informations recueillons-nous ?*, disponible sur: https://www.facebook.com/about/privacy/update (consulté le 27.06.2019), la politique d'utilisation des données Instagram, *quels types d'informations recueillons-nous ?*, disponible sur: https://fr-fr.facebook.com/help/instagram/155833707900388 (consulté le 27.06.2019), conditions d'utilisation Twitter, *vos droits et concession de droits sur le contenu,* disponible sur: https://twitter.com/fr/tos#current (consulté le 27.06.2019).
[6] PRAZ, p. 2.
[7] MÉTILLE, p. 55.

Les informations et données des utilisateurs représentent la source de revenus principale des services offerts généralement gratuitement sur le web. Les informations quant aux habitudes, aux comportements et aux centres d'intérêt des utilisateurs ont une réelle valeur[8]. Dans la perspective d'allouer davantage d'importance aux données, les utilisateurs font l'objet de suivi en permanence à l'aide d'outils performants dans le but de collecter leurs données, de les traiter et de les mettre à disposition d'annonceurs à des fins publicitaires.

3. Profil

Le profil se définit comme « un ensemble de données qui caractérise un individu ou une catégorie d'individus et qui est destiné à être appliqué à un individu »[9]. Un profil peut être *prédictif*. Il est établi à la suite de l'observation et de l'analyse des comportements, actions ou interactions d'une personne dans le temps, par exemple au travers des sites web visités, des mots-clés recherchés, des publicités avec lesquelles l'internaute a interagi[10]. Avec un mécanisme prédictif, le sexe, la tranche d'âge ou les centres d'intérêt sont déduits des actions et comportements de l'internaute[11]. Il peut également s'agir d'un profil *explicite*, établi sur la base des données que l'individu a lui-même fourni, notamment lors de son inscription à un réseau social[12]. En d'autres termes, un profil constitue le résultat d'une corrélation de données effectuée dans le cadre d'un profilage. Données qui, prises individuellement, peuvent s'avérer totalement ou partiellement anodines mais dont la combinaison permet d'aboutir à un profil précis[13].

4. Profilage

L'art. 4 par. 4 RGPD[14] définit le profilage comme « toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique ». Le profilage apparaît comme une technique particulière de traitement des données[15] et consiste en une analyse des comportements, des actions et interactions d'un individu provenant de sources différentes. Le but du processus est de déduire certaines caractéristiques ou révéler des informations non apparentes pour l'internaute mais qui lui sont inférées afin de lui attribuer un certain profil[16]. Ceci dans la perspective de prendre des décisions individuelles à son égard[17], de prédire ou d'influencer son comportement et ses choix[18].

---

[8] *Ibid*.
[9] WALTER, p. 95.
[10] GR29, WP171, p. 8. *Cf.* aussi: CNIL, p. 12 ss. ; WALTER, p. 95 ss.
[11] Par exemple: personne de sexe féminin, entre 15 et 35 ans, dont les intérêts sont l'art, la musique et le sport.
[12] GR29, WP171, p. 8. *Cf.* aussi: CNIL, p. 12 ; WALTER, p. 96.
[13] SARGSYAN, p.91 ; MEIER, p. 225.
[14] Règlement (UE) 2015/679 du Parlement européen et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données, cité: RGPD).
[15] WALTER, p. 102.
[16] KING/FORDER, p. 698. *Cf.* aussi: HILDEBRANDT, *Defining Profiling,* p. 18.
[17] GR29, WP251 rév.01, pp. 8-9. A noter qu'une décision automatisée peut être prise avec ou sans profilage, tout comme le profilage peut ou peut ne pas déboucher sur une décision automatisée.
[18] COMITÉ CONSULTATIF, pp. 3-5.

Il s'agit en outre d'un processus dynamique en vue d'aboutir à un résultat, contrairement à la notion de « profil » qui fait référence à un processus statique ou à un résultat de traitement[19]. L'analyse des comportements, des habitudes et des intérêts d'une personne à des fins de publicités ciblées constitue un des principaux domaines d'application du profilage.

Il convient de distinguer le profilage *abstrait* ou *de groupe* du profilage *spécifique.* La différence réside principalement dans le fait que le profilage *abstrait* n'est pas fondé sur des données à caractère personnel[20] mais sur des données anonymes ou anonymisées et qui, par conséquent, ne se rapporte pas à une personne identifiée ou identifiable. C'est du moins le cas en début de processus[21]. Le profilage *spécifique* résulte de l'analyse de données fournies par la personne concernée, sans inférence. En pratique, les profils ainsi générés résultent souvent d'une combinaison des profilages abstrait et spécifique[22]. Tel est le cas de la publicité ciblée sur les réseaux sociaux étant donné que les données collectées et analysées peuvent à la fois être livrées par l'utilisateur et être déduites suite à l'observation de ses comportements.

5. Data mining

Si la collecte massive de données est possible grâce aux différentes techniques de traçage, la performance du profilage telle qu'on la connaît aujourd'hui est possible grâce au *data mining* (littéralement: « forage de données »). Le *data mining* peut se définir comme « l'application des techniques de statistiques, d'analyse de données et d'apprentissage automatique *(statistical learning ou machine learning)* à l'exploration et à l'analyse sans *a priori* de grandes bases de données, en vue d'en extraire des informations nouvelles et utiles pour le détenteur de ces données »[23]. Le *data mining* s'avère être un outil important lorsqu'il s'agit de traiter de façon efficace des bases de données au volume considérable[24]. Permettant d'extraire « l'information cruciale » des masses de données, il participe entre autres à l'identification des individus les plus susceptibles de devenir client et à la personnalisation des pages de sites web ou des publicités, en fonction du profil de chaque internaute[25]. Ainsi, le *data mining* se révèle être un outil de prédiction et d'aide à la décision essentiel[26].

Le *data mining* permet en outre la constitution de profils encore plus riches grâce aux données issues des réseaux sociaux, au vu des activités déployées par les utilisateurs comme la description d'eux-mêmes, l'exposition de leurs centres d'intérêt et ceux de leurs amis[27]. Plus surprenant encore, certaines recherches portant sur l'analyse des comportements d'utilisateurs de réseaux sociaux démontrent qu'il est possible de prédire certains attributs personnels très sensibles, comme l'orientation sexuelle, l'origine ethnique, les opinions politiques et religieuses, la consommation de substances toxiques, etc., dans les cas où ces informations n'auraient pas été fournies par l'utilisateur[28].

---

[19] AUF DER MAUR/FEHR-BOSSHARD*,* p. 12.
[20] MEIER, p. 226.
[21] *Cf. infra* Partie 2, Ch. 1, A et B.
[22] COMITÉ CONSULTATIF, pp. 3-5.
[23] TUFFERY, *La science des données,* p. V. Ces « nouvelles informations » consistent, par exemple, en les préférences pour certains produits, les habitudes et comportements typiques. Pour en savoir plus sur le *data mining*, *Cf.* par exemple: TUFFERY, *L'intelligence des données*, p. 1 ss ; SCHWEIZER, *CRM*, p. 139 ss ; *idem*, *Data Mining*, p. 108 ss.
[24] COMITÉ CONSULTATIF, p. 10.
[25] *Ibid.*
[26] TUFFERY, *L'intelligence des données*, p. 1.
[27] *Ibid.*
[28] KING/FORDER, p. 700.

B. Publicité sur les réseaux sociaux

1. Généralités

Sur les réseaux sociaux, des publicités personnalisées, et donc susceptibles d'être intéressantes et pertinentes pour les utilisateurs, sont affichées. Celles-ci résultent de l'analyse de leurs activités en ligne[29]. Les services et produits proposés sont davantage susceptibles d'être achetés[30], puisqu'ils reflètent ce que les utilisateurs désirent, apprécient ou ont besoin. Une description du modèle économique type des réseaux sociaux, puis les types de publicités sont présentés dans cette section afin de rappeler l'origine des services publicitaires offerts par les réseaux sociaux et la raison de leur succès.

2. Modèle économique type

Le modèle économique type des réseaux sociaux repose sur deux éléments déterminants, qui sont la gratuité de l'accès et de l'utilisation de la plate-forme, d'une part, et la publicité, d'autre part. Aujourd'hui, les données sont considérées comme une matière première, une véritable mine d'or numérique. Il n'est plus question d'éthique s'agissant de leur utilisation mais d'économie et de stratégie, d'argent et de pouvoir[31]. C'est sur le modèle de la gratuité des services, à l'image du *Web 2.0*[32], que reposent les réseaux sociaux les plus populaires tels que Facebook, Instagram et Twitter. Les services publicitaires offerts par les réseaux sociaux consistent à utiliser les données à leur disposition dans le but de cibler les consommateurs potentiellement intéressés[33]. L'avantage pour l'annonceur est de bénéficier d'une audience ciblée, ce qui lui permet d'augmenter l'impact de son annonce[34]. Il s'agit en d'autres termes de la faculté de placer une annonce au bon endroit, au bon moment, face au bon utilisateur[35]. En général, le prix de ce service est défini par l'annonceur qui détermine le budget qu'il est prêt à débourser pour sa campagne publicitaire[36]. Un prix minimal peut être fixé par l'exploitant selon l'intensité du ciblage, l'annonceur ayant le choix entre plusieurs critères de ciblage tel que le sexe, le genre, la zone géographique et les centres d'intérêt. La qualité et la quantité des résultats obtenus par l'exploitant dépendent du prix fixé préalablement et du public cible défini par l'annonceur[37]. Les données traitées aux fins du ciblage ne sont ni vendues ni portées à la connaissance des annonceurs par les exploitants. Il en va de même de l'attribution des critères sélectionnés aux profils-utilisateurs[38].

---

[29] SARGSYAN, p. 10.
[30] *Ibid.*
[31] LEROY, p. 105.
[32] *Idem,* pp. 109-110. *Cf.* aussi: WAUTHY, pp. 3-4.
[33] ANTREASYAN, p. 22. Également: CATANESE ET AL., p. 3.
[34] WAUTHY, p. 5.
[35] LEROY, pp. 111-112.
[36] Twitter Business, *Tarification des Publicités Twitter,* disponible sur: https://business.twitter.com/fr/help/overview/ads-pricing.html (consulté le 02.07.2019) ; LinkedIn Marketing Solutions, *Combien coûtent les publicités LinkedIn,* disponible sur: https://business.linkedin.com/fr-fr/marketing-solutions/ads/pricing (consulté le 02.07.2019) ; Facebook Business, *Coût de la publicité sur Facebook,* disponible sur: https://www.facebook.com/business/help/201828586525529 (consulté le 02.07.2019). Les publicités sur Instagram sont créées à partir du gestionnaire de publicité Facebook, le processus de création et fixation du prix est donc le même.
[37] *Ibid.*
[38] La politique d'utilisation des données Facebook stipule sur ce point qu'aucune information permettant d'identifier personnellement un utilisateur est partagée avec les annonceurs. En revanche, des informations sur les types ou catégories de personnes ayant interagi avec leur publicité leur sont fournies (par exemple femme entre 25 et 34 ans) ; politique d'utilisation des données Facebook, *comment ces informations sont-elles partagées ?*,

La gratuité permet d'offrir un service accessible et destiné à un grand nombre d'utilisateurs. La publicité, quant à elle, est un service offert à des tiers à titre onéreux et permet d'obtenir un revenu. Il existe, dès lors, un lien intrinsèque entre la gratuité et la publicité. Ce procédé est au cœur du modèle économique type des réseaux sociaux d'aujourd'hui.

3. Publicité comportementale et personnalisée

La publicité comportementale repose sur l'observation et l'analyse des comportements en ligne dans le temps[39]. Le but est de déduire un profil spécifique à partir des caractéristiques retenues et analysées à travers le suivi de l'utilisateur, telles que la visite d'un site web, les mots-clés saisis, les interactions avec un certain contenu ou une publicité[40]. Le contenu publicitaire qui s'affiche est adapté aux centres d'intérêt ainsi déduits de l'utilisateur. La publicité personnalisée est une publicité choisie en fonction de certaines caractéristiques fournies par l'internaute comme son âge, son sexe ou sa localisation[41]. On parle parfois de *ciblage comportemental personnalisé* lorsque la publicité est fondée à la fois sur des caractéristiques communiquées par l'internaute et sur des centres d'intérêt inférés à la suite de l'observation et du suivi en ligne. Sur les réseaux sociaux, ce type de publicité est celui le plus utilisé.

Les types de publicités présentées ci-dessus se distinguent de la publicité contextuelle qui est choisie en fonction du contenu immédiat fourni à l'internaute, c'est-à-dire en fonction du contenu figurant sur la page sur laquelle l'internaute se trouve ou en fonction des mots-clés saisis par ce dernier dans un moteur de recherche[42]. La publicité contextuelle et comportementale se différencie au niveau de la temporalité. La publicité contextuelle repose sur un mécanisme *immédiat* en ce sens que son contenu est en adéquation avec la thématique de navigation de l'internaute sur le moment[43]. La publicité comportementale, quant à elle, s'inscrit dans la durée étant donné qu'elle découle d'un suivi dans le temps[44].

CHAPITRE 2: TRAITEMENTS DE DONNÉES À DES FINS DE CIBLAGE PUBLICITAIRE

A. Généralités

1. Des traitements de données à la fois services et contre-prestations

Le réseau social agit en tant que prestataire de services vis-à-vis des utilisateurs en leur permettant d'héberger, de publier et d'échanger des données sur la plate-forme et en leur octroyant un libre accès à cette dernière. À ce titre, le réseau social traite les données des utilisateurs pour fournir l'accès à la plate-forme, permettre son utilisation et s'assurer que les prestations attendues des utilisateurs et comprises dans le contrat d'utilisation soient réalisées[45].

---

disponible sur: https://www.facebook.com/about/privacy/update (consulté le 27.06.2019). Voir également le communiqué sur le fonctionnement de l'entreprise Facebook, disponible sur: https://www.facebook.com/business/news/mark-zuckerberg-shares-how-we-run-our-business/ (consulté le 02.07.2019).

[39] *Idem,* p. 75.

[40] JOUX, p. 52 ; CNIL, p.5 ; GR29, WP163, p. 10 ; *idem*, WP171, p. 5.

[41] CNIL, p. 5.

[42] JOUX, p. 52 ; CNIL, p. 5 ; GR29, WP163, p. 10.

[43] MERCANTI-GUÉRIN/VINCENT, p. 172.

[44] *Ibid.*

[45] *Cf.* SARGSYAN, p. 52 ss quant aux obligations de l'exploitant vis-à-vis de l'utilisateur.

Parallèlement, le réseau social effectue des traitements de données de ses utilisateurs pour son propre compte, soit dans le cadre de la vente de services publicitaires à des annonceurs tiers où les données sont traitées à des fins de ciblage publicitaire. Il s'ensuit que des traitements concernant potentiellement les mêmes données sont effectués à diverses fins, en faveur des utilisateurs d'une part et, en faveur des annonceurs d'autre part[46]. Par exemple, lorsqu'un utilisateur souhaite publier un contenu, l'exploitant devra faire en sorte que ledit contenu soit publié au moment et à l'endroit décidé par l'utilisateur. Les informations relatives à ce même contenu seront également stockées dans les bases de données servant au ciblage publicitaire, de sorte que l'utilisateur à l'origine de ce contenu pourrait être ciblé par une publicité jugée pertinente en regard du contenu préalablement publié. Toutefois, la présente section se concentre uniquement sur les données traitées à des fins publicitaires. Tout d'abord, les différentes opérations du processus menant au ciblage seront identifiées, puis le lecteur sera éclairé sur la manière dont les données sont collectées, pour terminer sur les diverses possibilités offertes aux annonceurs de cibler leurs publicités.

2. Opérations identifiées

L'importance d'identifier toutes les opérations du processus menant au ciblage publicitaire tient au fait qu'elles constituent chacune individuellement un traitement distinct de données. Dès lors, les responsables de traitement doivent satisfaire aux exigences en matière de protection des données lors de chacune des étapes identifiées. Le traitement de données à des fins de ciblage publicitaire recourt au profilage. Pour rappel, le profilage comporte trois étapes, à savoir l'observation en ligne et la collecte de données, l'analyse automatisée de ces données afin d'établir des corrélations, et enfin l'inférence à un individu de nouvelles caractéristiques ou variables comportementales déduites des corrélations[47]. Chacune de ces étapes constitue un traitement de données, de la collecte à l'attribution des nouvelles informations à un utilisateur contribuant à l'élaboration de son profil. Pour finir, l'opération par lequel les publicités sont diffusées auprès d'une audience spécifique, soit le ciblage, constitue la dernière étape du processus et doit aussi satisfaire aux exigences.

B. Collecte de données, profilage et ciblage publicitaire

1. Généralités

La capacité de ciblage est avant tout une question d'informations. Dans le but de satisfaire les demandes d'annonceurs, le réseau social collecte les données de ses utilisateurs tant à l'interne qu'à l'externe de sa plate-forme, que ces données aient été fournies volontairement par la personne concernée ou à la suite de l'observation de son comportement[48]. Toutes ces données servent à enrichir le profil des membres du réseau social et à cibler l'utilisateur.

[46] *Cf.* notamment *infra* Partie 1, Ch. 2, B, ch. 5 sur les mécanismes de ciblage proposés par les exploitants aux annonceurs et qui relate le mécanisme des services publicitaires relatif au ciblage.
[47] COMITÉ CONSULTATIF, p. 6 ; GR29, WP251 rév.01, pp. 7-8.
[48] Pour afficher une publicité relative à une compagnie aérienne affichée sur Facebook, le réseau social a aussi bien pu déduire cet intérêt à la suite d'un « Like » de l'utilisateur pour les pages d'un hôtel sur la plate-forme que la visite par cet utilisateur d'un site web d'un hôtel. Exemple tiré de SARGSYAN, p. 76.

L'avantage de la publicité sur les réseaux sociaux réside principalement dans le fait que le processus n'implique pas trois parties, comme c'est généralement le cas s'agissant de la publicité sur Internet, mais uniquement deux parties, à savoir l'annonceur et l'exploitant du réseau social, sans passer par un fournisseur de réseaux publicitaires[49]. Les données relatives aux comportements et aux actions de l'utilisateur sont collectées et analysées à l'aide des techniques de *traçage*, tels que les cookies et les pixels espions (ou *web-bugs*)[50]. Les informations recueillies, puis regroupées entre elles, permettent l'établissement de profils spécialement précis[51].

La liste des sources de collecte de données présentées ci-après est loin d'être exhaustive. En effet, établir de façon complète les sources de données collectées engendrerait un travail laborieux. Par conséquent, seules les sources de collecte de données les plus courantes ont été retenues.

2. Collecte de données à l'interne du réseau social

Par données collectées à l'interne au réseau social, on entend principalement les données partagées volontairement par l'utilisateur[52], notamment au moment de son inscription, lorsqu'il fournit des informations le concernant sur la page dédiée à son compte. Il s'agit là des informations du compte et du profil (2.1). Les informations concernant ses actions et comportements réalisés sur la plate-forme sont également pertinentes (2.2). Deux différences sont à opérer entre les informations du compte et du profil et les informations découlant des actions et comportements. Les informations de la première catégorie sont généralement statiques, rarement sujettes à des modifications et directement fournies par l'utilisateur[53]. Les informations de la deuxième catégorie sont quant à elles de nature dynamique, continuellement en mouvement et observées en temps réel[54].

2.1 Informations du compte et du profil

Lorsque l'utilisateur ouvre un compte, il doit en général fournir un nom, un prénom, une adresse mail, un mot de passe et une date de naissance. Une fois inscrit, l'utilisateur est invité à compléter son profil, par exemple en invitant certains de ses amis déjà présents sur la plate-forme, en ajoutant un numéro de téléphone, des informations concernant sa localisation géographique, son parcours professionnel ou scolaire, sa situation amoureuse ou une photo de profil[55]. Ainsi, l'exploitant du réseau social connaît de ses utilisateurs tout ce que ces derniers ont eux-mêmes fourni lors de leur inscription[56], voire par la suite en cas de modifications ou d'ajouts d'informations sur leur profil.

---

[49] SARGSYAN, p. 76 ; GR29, WP171, p. 6. En principe, un diffuseur réserve un espace dédié à de la publicité sur sa plate-forme ou son site web. Un ou plusieurs fournisseurs de réseaux publicitaires sont chargés du suivi des internautes, de la collecte de données, du profilage et distribuent les annonces au diffuseur. Les fournisseurs de réseaux publicitaires mettent en relation les diffuseurs et les annonceurs désireux de promouvoir une annonce auprès d'un public cible. Les réseaux sociaux sont souvent eux-mêmes équipés des services généralement fournis par les fournisseurs de réseaux publicitaires.
[50] SARGSYAN, p. 76.
[51] MÉTILLE, p. 13.
[52] LEROY. p. 113.
[53] JOLER/PETROVSKI, *Immaterial Labour,* disponible sur: https://labs.rs/en/facebook-algorithmic-factory-immaterial-labour-and-data-harvesting/ (consulté le 06.04.2019).
[54] *Ibid*.
[55] LEROY, p. 154.
[56] SCHLEIPFER, p. 322.

2.2 Actions et comportements

Les données ne sont pas fournies en tant que telles par l'utilisateur mais sont analysées dans le but d'en déduire des informations pertinentes à ajouter au profil-utilisateur. Ces informations proviennent par exemple des photos sur lesquelles l'utilisateur est identifié, de ses réactions à une publication tel qu'apposer un « J'aime », de sa messagerie instantanée, des commentaires, des réponses à des commentaires, de ses avis exprimés (sur une marque, un produit, un service, un film…), du temps passé sur une publication ou une page, des évènements auxquels l'utilisateur participe, des invitations déclinées, de ses centres d'intérêt, des applications installées, des interactions avec les publicités proposées, des articles partagés, etc.[57]. Il peut, par exemple, être déduit d'un « J'aime » à une publication concernant des voitures que l'utilisateur porte de l'intérêt sur tout ce qui a trait à l'automobile. À noter que les actions et comportements d'autres personnes sur la plate-forme, comme les amis de l'utilisateur, ont également pour effet d'alimenter les profils-utilisateurs[58]. Les informations retenues, recoupées aux données déjà en possession de l'exploitant[59], serviront à compléter le profil-utilisateur afin d'offrir de la publicité personnalisée en fonction de ce qui a pu être observé sur la plate-forme.

3. Collecte de données en dehors du réseau social

L'intérêt de collecter des données en dehors de la plate-forme est que cela permet d'enrichir considérablement le profil-utilisateur. Les pages web visitées peuvent révéler des informations quant à son emplacement, ses intérêts, ses achats, sa situation professionnelle ou même son état de santé[60]. Par données collectées à l'externe au réseau social, on entend principalement les données collectées à l'insu de utilisateur[61], c'est-à-dire déduites de certaines actions, interactions ou comportements en dehors de la plate-forme sociale dont il est membre, soit sur d'autres sites web ou applications[62].

Constituent des données collectées à l'externe de la plate-forme celles recueillies à l'aide des outils d'*online tracking* (3.1), tels que les cookies (3.1.1), les plugins sociaux (3.1.2) et les pixels (3.1.3), les données de géolocalisation (3.2), les informations concernant le dispositif de l'utilisateur (3.3) et les autorisations d'accès octroyées aux applications par l'appareil mobile (3.4). Enfin, la problématique des courtiers en données en lien avec Facebook sera brièvement invoquée afin d'avoir une idée du rôle non négligeable des applications tierces au sein d'un réseau social (3.5).

3.1 Collecte au travers des « online trackers »

Les « online trackers » (ou outils de suivi en ligne) sont des mécanismes utilisés pour suivre l'activité des internautes sur le web, observer leurs comportements en ligne[63] et conserver leur historique de navigation. Trois outils seront successivement présentés dans le présent chapitre: les cookies (3.1.1), les plugins sociaux (3.1.2) et les pixels (3.1.3).

[57] LEROY, p. 55 ss ; SÖBBING, p.182 ; ANDREOU ET AL., p. 4.
[58] LEROY, p. 155.
[59] *Ibid*.
[60] MAYER/MITCHELL, p. 415.
[61] LEROY, p. 113.
[62] ANDREOU ET AL., p. 4.
[63] LEONARD, p. 3.

3.1.1 Cookies

Le cookie est un petit fichier de données transmis par le serveur web visité par l'internaute au logiciel de navigation et dont une copie est sauvegardée dans le navigateur[64]. Le site web visité par l'internaute dépose un code d'identification sur le dispositif de l'utilisateur[65]. Le cookie est codé, inintelligible pour l'internaute et sa durée de vie varie selon ce que le serveur à la source a décidé[66]. Il est relié à un navigateur et non pas à l'internaute[67]. Lors d'une connexion ultérieure, le serveur accède aux informations préalablement enregistrées dans le cookie, ce qui lui permet d'identifier l'utilisateur[68]. Ainsi, le cookie offre la possibilité de réunir toutes les informations antérieurement enregistrées, comme l'identifiant unique attribué à l'internaute, les préférences de paramètre du site, l'adresse IP, l'entité qui a déposé le cookie, les informations que l'internaute a lui-même fournies au site web comme son adresse e-mail[69], avec celles qui le seront ultérieurement. Ce procédé permet de suivre l'historique de navigation[70], de garder une trace de leurs habitudes et d'établir des profils détaillés.

Les cookies placés sur un site web par un tiers différent du propriétaire du site web sont appelés « cookies tiers » ou « third party cookies »[71]. Les « cookies d'origine » sont ceux mis en place par l'exploitant de la page web visitée par l'utilisateur[72]. Ainsi, un réseau social reconnaît ses utilisateurs grâce à ses cookies placés sur des sites web tiers[73] et récolte les informations qui y sont stockées. Il est utile d'opérer à une distinction entre les cookies *nécessaires* et ceux qui ne le sont pas. Les cookies *nécessaires* sont ceux requis pour fournir une fonctionnalité spécifique à l'utilisateur[74]. En cas de désactivation de ce cookie, ladite fonctionnalité ne sera pas ou plus disponible[75]. Les cookies tiers ne sont en principe pas strictement nécessaires, ceux-ci n'étant généralement pas reliés au service demandé par l'utilisateur[76] mais intégrés au site web dans un but statistique ou publicitaire.

Une autre distinction utile est celle entre les « cookies de session » et les « cookies persistants ». Les premiers sont automatiquement supprimés lorsque l'internaute ferme son navigateur[77], contrairement aux seconds qui restent stockés sur son dispositif jusqu'à une date d'expiration prédéfinie[78]. Le cookie de session est en principe fondé sur un identifiant de session, c'est-à-dire un numéro unique temporaire qui expire à la fin de la session, voire avant.

---

[64] SCHWEIZER, *CRM,* p. 294.
[65] *Ibid*.
[66] LEONARD, p. 4
[67] MÉTILLE, p. 12.
[68] SCHWEIZER, *CRM,* p. 294.
[69] EBERSOHN, pp. 742-743.
[70] ESTEVE, p. 39.
[71] GR29, WP171, p. 7.
[72] *Ibid*.
[73] SCHLEIPFER, p. 323.
[74] GR29, WP194, p. 2. Cette distinction est importante s'agissant du consentement. En effet, les cookies strictement nécessaires sont exemptés de consentement s'ils visent exclusivement à effectuer la transmission d'une communication par la voie d'un réseau de communication ou s'ils sont strictement nécessaires pour la fourniture d'un service expressément demandé par l'utilisateur. Sont exclus de cette exemption, faute d'être strictement nécessaires, les cookies utilisés à des fins de suivi de l'utilisateur dans le but de présenter de la publicité personnalisée ou ciblée.
[75] *Ibid.*
[76] *Idem,* p. 5.
[77] SCHWEIZER, *CRM,* pp. 295-296.
[78] *Ibid*. *Cf.* aussi: GR29, WP194, p. 4 ss.

Il est en général alimenté par l'utilisateur pour conserver des informations saisies par lui-même (par exemple le panier d'achats). Les cookies alimentés par l'utilisateur sont des cas typiques de cookies nécessaires, puisqu'ils sont expressément demandés par ce dernier, tout comme les cookies d'authentification utilisés pour identifier l'utilisateur dès qu'il se connecte ou fait une demande d'accès ou encore les cookies de personnalisation de l'interface utilisateur utilisés pour mémoriser par exemple la préférence linguistique.

3.1.2 Plugins sociaux

Les exploitants de sites web ont la possibilité d'utiliser sur leurs propres sites certains services de réseaux sociaux, comme les plugins sociaux[79]. Les boutons « J'aime » ou « Partager » de Facebook sont sans doute les plus connus. Au moyen de ces plugins sociaux, les internautes ont la possibilité de partager le contenu d'un site web externe à la plate-forme sociale directement sur son profil au sein de la plate-forme ou uniquement avec certains amis également membres du réseau social[80]. Tout comme les cookies, les plugins sociaux intégrés sur des sites web permettent la transmission d'informations d'un visiteur, tels que son adresse IP, l'adresse du site web visité, la date et l'heure de la visite, le navigateur utilisé, sans qu'il ait eu besoin de cliquer sur le plugin et même si la personne concernée n'est pas membre ou n'est pas connectée au réseau social au moment de la visite[81].

La simple existence du plugin sur le site web visité enrichit la base de données utile à la constitution de profils d'utilisateur. En revanche, si l'utilisateur est en même temps connecté au réseau social pendant qu'il visite le site web, les données collectées seront directement mises en relation avec son profil-utilisateur déjà constitué[82]. S'il clique sur le bouton « J'aime », les informations concernant le contenu « aimé » seront également transmises[83]. Lorsqu'un utilisateur clique sur un plugin social, une inscription de cette interaction sera générée aussi bien sur le profil-utilisateur (c'est-à-dire le profil détenu par l'exploitant du réseau social et enrichi par ce dernier) que sur la page de l'utilisateur au sein de la plate-forme[84].

Les plugins sociaux étant des services externes, les exploitants de sites web ne peuvent pas en *suivre* l'utilisation[85]. En revanche, l'exploitant du réseau social peut suivre l'utilisation de ses plugins sociaux placés sur des sites web tiers, puisqu'il s'agit d'un service qu'il leur appartient et dont ils en ont la gestion[86]. Les sites web possédant de tels plugins sociaux n'ont pas beaucoup à y gagner, si ce n'est d'avoir la possibilité que les visiteurs recommandent lesdites pages web à d'autres personnes et d'ainsi faire de la publicité à leur égard[87].

---

[79] MAYER/MITCHELL, p. 419.
[80] Pour en savoir plus sur les fonctionnalités des plugins-sociaux Facebook, voir: SCHLEIPFER, p. 319.
[81] PRAZ, p. 8 ; ROGOSCH, p. 182.
[82] PFPDT: *Explications concernant le webtracking*, disponible sur: https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/Internet_und_Computer/webtracking/explications-concernant-le-webtracking.html.
[83] *Ibid.*
[84] SCHLEIPFER, p. 321. A titre d'exemple, les conditions d'utilisation Facebook stipule que lorsqu'on utilise le bouton « Commenter » ou « Partager » de Facebook sur un site web, le site web peut recevoir un commentaire ou un lien que l'on partage depuis son site web sur Facebook ; Politique d'utilisation Facebook, disponible sur https://www.facebook.com/policy.php (consulté le 05.04.2019).
[85] *Idem*, p. 320.
[86] *Idem,* pp. 320-321.
[87] *Idem*, p. 319.

En effet, les propriétaires de ces sites web n'ont pas accès aux informations recueillies sur l'internaute ayant adopté un comportement actif avec le plugin social, ni n'en recueillent[88]. Néanmoins, certains réseaux sociaux proposent aux exploitants de sites web qui ont intégré un plugin sur leur site un service analytique[89]. Ce service permet d'analyser le comportement des membres du réseau social sur leur site web et d'obtenir des statistiques d'utilisation, telles que la répartition par genre, par âge ou par pays[90].

3.1.3 Pixels

En vertu des possibilités offertes aujourd'hui aux internautes de limiter l'usage des cookies, les exploitants de sites web, les agences de marketing et les réseaux sociaux utilisent la technologie des pixels pour récolter des données. Les pixels, aussi connus sous le nom de pixel espion, balise web ou web bug, sont de très petites images numériques transparentes intégrées dans des pages web et dont il est plus difficile que les cookies de s'en soustraire[91]. Lorsqu'un internaute visite une page web, le pixel enregistrera que la page web a été ouverte par cet internaute ainsi que d'autres informations telles que l'adresse IP, l'URL du site web visité, la date, l'heure, la durée de la visite et le navigateur utilisé[92]. Ces informations permettent d'identifier l'utilisateur, de suivre son activité et d'obtenir des informations qui seront utilisées pour établir des profils[93].

3.2 Informations de localisation

La localisation des personnes concernées est une source importante d'informations en termes de publicités ciblées car elle permet une diffusion auprès de personnes qui se trouvent à un endroit précis ou dans les alentours. Les informations de connexion comme que l'adresse IP, la connexion WI-FI, la fonctionnalité Bluetooth[94] ou les informations de localisation telles que le signal GPS du dispositif offrent la possibilité de savoir où un utilisateur se trouve. Précisons que lorsqu'un utilisateur installe une application sur son appareil, celle-ci lui demande s'il l'autorise à le localiser[96].

---

[88] *Idem,* p. 320.
[89] Facebook Analytics, https://analytics.facebook.com (consulté le 05.04.2019).
[90] SCHLEIPFER, p. 322 ; KARG/THOMSEN, pp. 731-732.
[91] SCHWEIZER, *CRM,* pp. 298-299.
[92] *Idem,* pp. 300-301.
[93] *Ibid.*
[94] Pour davantage d'informations, voir: KETTIGER, N 7, CHARLET, p. 94 ss. Mentionnons également l'existence du *beacon* principalement utilisé pour le marketing mobile. Le beacon, technologie basée sur le *Bluetooth Low Energy* (technique de transmission sans fil dotée d'une consommation d'énergie nettement inférieure au Bluetooth classique), est une petite balise placée en général dans un lieu physique et qui émet des signaux qui seront détectés par l'appareil mobile. La détection de ces signaux permettra ainsi à une application mobile de déterminer la zone dans laquelle se trouve l'appareil. En d'autres termes, le beacon sert à signaler sa présence à un appareil mobile. Par exemple, l'application mobile d'une enseigne peut réagir à la détection de signaux transmis par un beacon à proximité d'un magasin de cette enseigne. L'appareil mobile sera ensuite susceptible de recevoir une notification, une publicité ou une promotion sur un produit de cette enseigne. À propos de cette technologie, *cf*. notamment: BÖPPLE/GLENDE/SCHAUBER, pp. 299-307.
[96] CHARLET, pp. 94-95.

Par la suite, l'utilisateur a en principe la possibilité de choisir via les *services de localisation* disponibles sur les paramètres de son téléphone mobile[97] s'il souhaite ou pas le partage de sa localisation avec l'application, soit le réseau social[98]. Toutefois, même si l'utilisateur choisit de ne pas autoriser un tel partage d'informations, le réseau social peut déterminer sa position grâce aux évènements auxquelles il participe, aux données concernant sa connexion Internet ou de son adresse IP[99]. Certaines applications ont également recours au micro de l'appareil mobile dans le but d'écouter des ultrasons émis dans les espaces publics et d'ainsi localiser les utilisateurs[100]. Le *data mining* permet en outre d'analyser la répétition ou le fait qu'un utilisateur se trouve au même endroit à une certaine heure de façon répétitive pendant la semaine pour ensuite déterminer où l'utilisateur vit et travaille ou s'il est actuellement à l'étranger[101].

3.3 Informations du dispositif

Le *device fingerprinting* (ou empreinte du dispositif, aussi appelé *browser fingerprinting* ou *machine fingerprinting*[102]) identifie les internautes en fonction de la configuration de leur dispositif ou de leur navigateur[103]. La différence principale avec le cookie est que le *device fingerprinting* ne stocke pas d'identifiant sur l'ordinateur de l'utilisateur. Le stockage des informations a lieu côté serveur, dans des bases de données[104]. Les empreintes du dispositif sont créées par la collecte de plusieurs types de données, notamment l'adresse IP, les informations du dispositif de l'internaute comme la résolution de son écran, le système d'exploitation, la langue, la police installée, l'heure, le fuseau horaire, etc.[105]. Ce sont autant d'éléments qui, selon leurs combinaisons, rendent un dispositif unique et identifiable.

Ces empreintes apparaissent comme une alternative aux cookies, dans la mesure où les cookies peuvent être supprimés par l'internaute. Il est ainsi possible d'identifier ce dernier sur la base de l'empreinte de son dispositif précédemment déterminée, indépendamment de la suppression de cookies. Lorsque la technique du *device fingerprinting* est utilisée en combinaison avec des cookies ou d'autres outils de suivi, l'exactitude de l'identification de l'internaute est fortement améliorée[106]. Par ailleurs, l'identification est d'autant plus facile également lorsque des extensions de protection de confidentialité ont été installées sur le navigateur (par exemple Ghostery ou Do Not Track Me), car cela causera une configuration davantage unique[107].

---

[97] Si l'utilisateur n'a pas installé l'application sur son téléphone, le réseau social ne reçoit pas d'informations de localisation en provenance de l'appareil mobile. Ajoutons qu'il existe une fonctionnalité appelée « localisation à l'arrière plan » qui permet au réseau social d'accéder aux données de localisation fournies par l'appareil mobile quand bien même l'utilisateur ne fait pas usage de l'application. Il est ainsi possible de permettre au réseau social d'accéder à la localisation de manière général ou uniquement lorsqu'il utilise l'application. La possibilité d'activer ou de désactiver « la localisation à l'arrière plan » s'opère directement depuis l'application, contrairement aux services de localisation dont les paramètres se trouvent sur l'appareil.

[98] CHARLET, pp. 94-95.

[99] WALTER, p. 91.

[100] MOHIT, *Hundreds of Apps Using Ultrasonic Signals,* disponible sur: https://thehackernews.com/2017/05/ultrasonic-tracking-signals-apps.html (consulté le 27.02.2019).

[101] JOLER/PETROVSKI, *Quantified Lives,* disponible sur: https://labs.rs/en/quantified-lives/ (consulté le 06.04.2019).

[102] ZAWADZIŃSKI/WLOSIK, *What Is Device Fingerprinting,* disponible sur: https://clearcode.cc/blog/device-fingerprinting/ (consulté le 31.03.2019).

[103] MATHYS/MEIER, p. 156.

[104] *Ibid.*

[105] *Ibid.*

[106] ZAWADZIŃSKI/WLOSIK, *What Is Device Fingerprinting,* disponible sur: https://clearcode.cc/blog/device-fingerprinting/ (consulté le 31.03.2019).

[107] BOUMANS, p. 15.

3.4 Autorisations des téléphones mobiles

Les applications téléchargées sur les appareils mobiles sont autorisées, généralement par défaut, à accéder à différentes informations stockées sur l'appareil[108]. Il peut s'agir de l'accès à la localisation précise de l'appareil, au carnet d'adresses, aux SMS et appels, au microphone, à l'appareil photo et aux photos, au calendrier et aux contenus téléchargés[109]. Ainsi, lorsque la version mobile d'une plate-forme sociale est téléchargée, l'exploitant a généralement accès aux diverses informations stockées si l'utilisateur ne modifie pas, de lui-même, ses paramètres de configuration directement sur son appareil.

3.5 Facebook : les problématiques liées aux « 3rd-Party App »

Durant son audition devant le Sénat américain au mois d'avril 2018, Mark Zuckerberg a affirmé que Facebook ne vendait pas de données personnelles concernant ses utilisateurs. Cependant, bien que le réseau social ne vende pas de données, il n'en reste pas moins que des applications tierces accessibles via Facebook peuvent collecter des données des utilisateurs lorsque ceux-ci font usage de l'application. Ce système a pour conséquence la perte de maîtrise par Facebook sur les données de ses utilisateurs, étant donné que ces applications sont exécutées à partir de serveurs externes. Ainsi, à moins d'en indiquer le contraire, l'utilisateur qui télécharge l'application tierce par le biais de la plate-forme sociale autorise l'application tierce à accéder aux données de son profil-utilisateur public et à celles de ses amis ainsi qu'à d'autres informations telles que le sexe, la langue et la tranche d'âge[110]. Une fois les données d'utilisateurs acquises via le réseau social, certains développeurs d'applications tierces malveillants vendent soit les données en tant que telles, soit l'application dans son entier à des *« data brokers[111]»* ou des compagnies de marketing. De telles manœuvres sont réalisées bien que la vente des données à d'autres compagnies ou data brokers soit interdite par les politiques d'utilisation de Facebook[112]. Les applications tierces accessibles via Facebook[113] (aussi appelées Facebook App) apparaissent comme de véritables chevaux de Troie créées afin d'obtenir l'accès aux profils des utilisateurs qui pourront être revendus par la suite[114].

---

[108] JOLER/PETROVSKI, *Immaterial Labour*, disponible sur: https://labs.rs/en/facebook-algorithmic-factory-immaterial-labour-and-data-harvesting/ (consulté le 06.04.2019).

[109] *Ibid*.

[110] Ces données sont ensuite utilisées pour retrouver des amis utilisant également l'application, personnaliser le contenu de l'application, faciliter le partage de contenus avec d'autres utilisateurs de la plate-forme Facebook ou encore faciliter la création d'un compte ; Facebook, *paramètres de confidentialité des applications et de vos informations,* disponible sur: https://www.facebook.com/help/262314300536014 (consulté le 26 juin 2019).

[111] Les data brokers (littéralement: courtiers en données ou fournisseurs de données) sont des entreprises qui collectent des données sur des centaines de millions de consommateurs, les analysent et les vendent généralement sans leur permission. Leur clientèle comprend tous les principaux secteurs industriels qui achètent ces données dans divers buts, que ce soit la prévention de la fraude, l'évaluation d'un crédit ou le marketing. Voir: U.S SENATE COMMITTEE, p. i.

[112] Facebook for developers, Politique de la plate-forme Facebook **ch. 2.4:** « *(…) les données d'utilisateurs obtenues de notre part ne peuvent pas être transférées à un courtier en données ni être vendues, même si vous le mentionnez dans votre politique de confidentialité (…)* », **ch. 3.9:** « *Ne vendez et n'achetez aucune donnée obtenue de nous ou de nos services, et n'octroyez aucune licence à ce sujet.* », **ch. 3.19:** *« Ne transférez, (…), aucune donnée que vous recevez de nous (y compris les données anonymes, agrégées ou dérivées) à un réseau publicitaire, un courtier en données ou un autre service en rapport avec la monétisation ou la publicité (…). »,* disponible sur: *https://developers.facebook.com/policy/?locale=fr_FR*, (consulté le 11.02.2019).

[113] On peut citer à titre d'exemple les petits jeux, les quiz, les tests de QI et les tests de personnalités.

[114] C'est notamment ce qui s'est passé avec Cambridge Analytica, société d'analyse de données basées à New-York, pour la campagne de Donald Trump en 2016. Pour en savoir plus sur le scandale Cambridge Analytica, voir: SÖBBING, p. 182 ss.

Il s'agit d'un *business model* méconnu du grand public et selon lequel les applications sont créées pas des développeurs externes dont le but est souvent, d'une part, de récolter des profils d'utilisateurs et, d'autre part, de les revendre. Suite au scandale Cambridge Analytica, Facebook ne permettrait plus à des développeurs tiers de récolter des données de la même manière. Des changements ont été opérés pour une meilleure protection des données des utilisateurs, en particulier s'agissant de l'utilisation des API[115] destinés aux développeurs[116].

Hormis cette problématique qui nécessiterait un travail plus approfondi, l'importance des applications tierces en termes de publicités ciblées réside dans le fait que les développeurs externes sont appelés, en théorie, à demander l'autorisation des utilisateurs afin de permettre à Facebook de collecter les données depuis l'application et de les utiliser à des fins de publicités ciblées[117]. Si une telle autorisation est donnée, cela a pour conséquence d'enrichir la base de données et d'apporter davantage de précision dans le ciblage publicitaire.

4. Profilage et constitution de profils

Le groupe de travail « article 29 »[118] a distingué trois domaines d'application du profilage. Il y a d'abord le profilage au sens large ou général qui implique un traitement automatisé aux fins d'analyser et prédire des comportements ou caractéristiques. Le groupe identifie ensuite la prise de décision fondée sur le profilage[119] et enfin la prise de décision « exclusivement » automatisée, y compris le profilage, qui produit des effets juridiques ou affecte de manière significative de façon similaire la personne concernée au sens de l'art. 22 RGPD[120]. Plus particulièrement, le profilage comporte plusieurs étapes: l'observation massive des comportements et la collecte de données en provenance de nombreuses sources, l'analyse de ces données et la création de corrélations entre certains comportements qui contribuent à l'établissement d'un profil et enfin l'inférence à un individu des nouvelles informations déduites des corrélations[121].

---

[115] Les *Application Programming Interface* ou API (littéralement: interface de programmation) sont des interfaces à disposition des développeurs qui leur permettent l'accès aux données personnelles d'utilisateurs. Les API ne sont pas à confondre avec les *Software Development Kit* ou SDK (littéralement: kit de développement) qui sont des logiciels à disposition des développeurs et qui leur permet de développer leur application sur la plate-forme.

[116] Facebook soumet les développeurs à une autorisation et à un examen plus approfondi de l'application avant de pouvoir utiliser un API. Les applications inactives ont une interdiction d'accès aux API. Consulter les communiqués de Facebook: https://developers.facebook.com/blog/post/2018/07/31/facebook-app-review-update/?ref=dev_banner (consulté le 11.02.2019) https://developers.facebook.com/blog/post/2019/01/28/deadline-rerequest-api-permissions/ (consulté le 11.02.2019).

[117] Facebook for developers, Politique de la plate-forme Facebook **ch. 2.8 let a:** « vous *(...) fournissez un avis approprié indiquant: que des tiers, notamment Facebook, sont susceptibles d'utiliser des cookies, des balises web et d'autres technologies de stockage pour recueillir ou recevoir des informations depuis vos sites web, vos applications et d'autres emplacements sur Internet, et d'utiliser ces informations pour fournir des services de mesure, des publicités ciblées (...)* », disponible sur: *https://developers.facebook.com/policy/?locale=fr_FR* (consulté le 11 février 2019).

[118] Le groupe de travail « article 29 » (abrégé GR29) est un ancien organe consultatif indépendant de l'Union européenne sur les questions de protection des données. Il a été établi en vertu de l'art. 29 de la directive européenne sur la protection des données. Dès l'entrée en vigueur du Règlement général sur la protection des données (RGPD), il a été remplacé par le Comité européen de la protection des données (abrégé CEPD).

[119] La décision est ici prise par un être humain sur la base d'un profil constitué par des moyens automatisés.

[120] Art. 22 par. 1 RGPD. La décision est dans ce cas prise sur la base d'algorithmes, sans intervention humaine préalable.

[121] GR29, WP251 rév.01, pp. 7-8 ; *idem,* p. 13. *Cf.* aussi: BEELEN, p. 174 ; BYGRAVE, p. 17.

Comme mentionné dans un chapitre ci-avant[122], le *data mining* rend possible l'interconnexion et la combinaison des données entre elles[123]. De plus, il facilite l'élaboration de profils précis, des centres d'intérêt et des activités des internautes.[124] Les données livrées directement par l'utilisateur, par exemple au moment de son inscription, sont rassemblées avec les données récoltées à l'externe et à l'interne de la plate-forme. La collecte, la combinaison de données et enfin leur réunification permettent d'enrichir les bases de données et d'affiner les profils-utilisateurs et par conséquent le ciblage publicitaire. Il est en outre possible pour le réseau social, sur la base de l'ensemble des éléments qu'il a en sa possession, de prédire quelle publicité est potentiellement susceptible d'intéresser un utilisateur.

5. Mécanismes de ciblage proposés

Le nombre considérable d'individus présents aujourd'hui sur les plates-formes sociales est un motif non négligeable pour lequel les annonceurs recourent aux services publicitaires offerts par les réseaux sociaux, donnant ainsi la possibilité d'atteindre une audience efficace. Ainsi, les résultats des opérations précédentes, soit le profilage, servent au ciblage publicitaire puisque les profils ainsi enrichis permettent un ciblage plus précis. En plus de cela, les services créés par les réseaux sociaux permettent aux annonceurs non seulement d'acheter des espaces publicitaires directement sur leur plate-forme, mais aussi de sélectionner l'audience voulue[125]. Les annonceurs ont la possibilité de déterminer le budget, la durée de diffusion des annonces et la taille de l'audience souhaitée, de même que la manière dont leur contenu publicitaire s'affiche sur la plate-forme. Ces services publicitaires s'étendent en principe sur toutes les applications et services appartenant au réseau social[126]. Ce dernier se charge d'afficher la publicité auprès du public cible choisi en appliquant les techniques de profilage et en se fondant sur toutes les informations qu'il a en sa possession.

5.1 Création d'une audience classique ou personnalisée

Pour afficher de la publicité ciblée, résultat d'un processus de profilage et d'analyse comportementale, les annonceurs ont la possibilité de sélectionner des critères de ciblage permettant de définir une audience cible spécifique[127]. Outre la sélection de critères, les annonceurs doivent également spécifier un prix et un objectif publicitaire, qui précise le résultat escompté par la diffusion des annonces[128]. Ensuite, le processus de ciblage vérifie les concordances entre les critères sélectionnés et les utilisateurs[129].

Parmi les critères de ciblage proposés figurent le lieu, le sexe, la tranche d'âge, la langue. Pour affiner davantage le public cible visé, des critères de ciblage avancé sont proposés[130]. Ceux-ci sont généralement répartis en trois catégories, à savoir les centres d'intérêt, le comportement et les informations démographiques.

---

[122] *Supra* Partie 1, Ch. 1, A, ch. 5.
[123] MEIER, p. 225.
[124] GR29, WP163, p. 4.
[125] SARGSYAN, p. 7.
[126] Sur Facebook par exemple, grâce au service « d'optimisation des placements », l'annonceur peut atteindre son public cible sur Facebook, Instagram, l'Audience Network et Messenger.
[127] SARGSYAN, p. 76.
[128] ANDREOU ET AL., p. 3.
[129] *Ibid.*
[130] *Ibid.*

Il est ainsi possible pour un annonceur de soumettre toute proposition qu'il juge utile pour sa campagne avec des critères comme « parent (intérêt) », « parent de jeunes enfants (données démographiques) », ou encore « parti politique (intérêt) », « interaction probable avec du contenu politique (comportement) », « religion (intérêt) » ou « attraction sexuelle (intérêt) ». Les réseaux sociaux permettent donc de cibler les utilisateurs à partir de caractéristiques précises et potentiellement sensibles[131].

À côté de l'audience classique, les annonceurs peuvent créer une audience personnalisée[132] qui permet de préciser les cibles souhaitées[133]. Il existe principalement deux façons de personnaliser une audience. La première consiste en la possibilité pour les annonceurs de télécharger une liste de renseignements personnels, comme les adresses électroniques, les adresses postales ou les numéros de téléphone des utilisateurs qu'ils souhaitent atteindre[134]. Les informations téléchargées par les annonceurs sont hachées[135], puis comparées aux données d'utilisateurs pour détecter une correspondance[136]. La fonction de hachage permet à l'exploitant de ne pas avoir connaissances des données ainsi fournies, puisque celles-ci sont instantanément converties en empreintes numériques (souvent une suite de chiffres et de lettres) qui l'empêchent de pouvoir lire ces données. Ces empreintes numériques sont ensuite comparées aux empreintes déjà stockées sur les serveurs de l'exploitant dans le but de trouver une concordance et conclure à la présence ou non d'une donnée. Le but du hachage est donc de pouvoir comparer des données (les empreintes) sans pour autant avoir la possibilité de les lire[137]. Si les annonceurs recourent à la création d'une audience personnalisée, le réseau social ciblera uniquement les utilisateurs figurant dans la liste préalablement fournie, sans toutefois leur révéler l'identité des membres concordants[138]. La seconde manière de personnaliser une audience est de cibler uniquement les utilisateurs ayant préalablement interagi avec le site web[139] ou l'application[140] de l'annonceur. Seront ciblées, par exemple, les personnes ayant déjà acheté des produits ou passé commande auprès de l'entreprise à l'origine de l'annonce diffusée, raison pour laquelle celui-ci est d'ores et déjà en possession d'informations sur cet utilisateur.

---

[131] HOOFNAGLE ET AL., p. 276. Certains critères relèvent de données appartenant aux catégories particulières de données à caractère personnel au sens de l'art. 9 RGPD, respectivement de données sensibles au sens de l'art. 3 let. c de la LF du 19 juin 1992 sur la protection des données (= LPD ; RS 235.1).

[132] Audience personnalisée sur Facebook: https://www.facebook.com/business/help/744354708981227 (consulté le 04.04.2019); sur LinkedIn: https://business.linkedin.com/fr-fr/marketing-solutions/ad-targeting? (consulté le 04.04.2019) ; sur Twitter: https://business.twitter.com/fr/targeting/tailored-audiences.html (consulté le 04.04.2019).

[133] LEROY, p. 167.

[134] ANDREOU ET AL., p. 3.

[135] OBERLIN, *Teil 2,* p. 68. Imaginons le cas d'un bijoutier qui souhaite qu'uniquement les personnes déjà inscrites à sa newsletter et membres de la plate-forme soient ciblées par ses publicités. Il téléchargera sa liste d'adresses électroniques. Ces adresses seront instantanément hachées. Ces données hachées seront ensuite recoupées avec la liste d'adresses électroniques également hachées et associées à des comptes d'utilisateurs de la plate-forme. Le hachage n'équivaut pas à un processus d'anonymisation car les utilisateurs restent identifiables suite à une correspondance. Les données hachées ont en outre été qualifiées de données personnelles par le Tribunal administratif de Bayreuth dans une décision du 8 mai 2018 - B 1 S 18. 105, N 8 et N 45.

[136] *Ibid*.

[137] Voir : HADMI, pp. 33-45.

[138] ANDREOU ET AL., pp. 3-5. Facebook exige désormais des annonceurs qu'ils garantissent que les données-clients déjà en leur possession et téléchargées pour le ciblage publicitaire aient été récoltées avec leur consentement. Voir: Facebook Business, *Introducing New Requirements for Custom Audience Targeting,* disponible sur: https://www.facebook.com/business/news/introducing-new-requirements-for-custom-audience-targeting (consulté le 04.04.2019).

[139] Lorsqu'un annonceur installe un pixel sur son site web, le réseau social attribue instantanément au visiteur son identifiant d'utilisateur, de sorte qu'il est possible de cibler sur la plate-forme uniquement les visiteurs du site web.

[140] L'annonceur doit préalablement inscrire son application sur le SDK du réseau social pour pouvoir cibler les personnes ayant installé leur application (*infra* nbp 114).

Il convient d'ajouter qu'en plus des données récoltées à l'interne et à l'externe de leur plate-forme, les exploitants recourent également à des données fournies par des *data brokers*[141]. Ces derniers collaborent avec les réseaux sociaux et mettent leurs données à disposition de ceux-ci, ce qui permet d'élargir la source d'informations pouvant servir au ciblage publicitaire[142].

5.2 Audience Network

L'Audience Network[143] concerne les publicités diffusées en dehors des plates-formes, sur d'autres sites web et applications qui utilisent les technologies des réseaux sociaux. La possibilité est ainsi offerte aux annonceurs de diffuser leurs publicités auprès d'une audience plus large. Les publicités de l'Audience Network emploient les mêmes systèmes de ciblage et de diffusion que les publicités à l'interne des plates-formes. La diffusion se fait en collaboration avec des éditeurs qui ont la possibilité de gérer la façon dont une annonce va s'afficher sur leur site web ou leur application[144]. Ces éditeurs sont préalablement sélectionnés par l'exploitant qui vérifie leur conformité aux exigences requises.

PARTIE 2: BASE JURIDIQUE LÉGITIMANT LE TRAITEMENT DE DONNÉES À DES FINS DE CIBLAGE PUBLICITAIRE

CHAPITRE 1: APPLICABILITÉ DE LA LÉGISLATION SUR LA PROTECTION DES DONNÉES

Pour déterminer si les données traitées à des fins de ciblage publicitaire tombent ou non sous l'application de la législation sur la protection des données, il sera examiné dans le présent chapitre les notions de « données à caractère personnel concernant une personne identifiée ou identifiable » (A), puis ce qu'il en est concernant les données traitées à des fins de ciblage publicitaire (B). Le deuxième chapitre sera consacré à la question de la licéité du traitement.

A. Données à caractère personnel concernant une personne identifiée ou identifiable

L'art. 4 par. 1 RGPD définit les données à caractère personnel comme « toute information se rapportant à une personne physique identifiée ou identifiable »[145]. Il faut que la donnée *concerne* la personne en cause.

---

[141] *Cf.* supra nbp 111 ; ANDREOU ET AL., p. 5. Facebook a décidé en mars 2018 de retirer la possibilité à des courtiers en données d'offrir leur ressources en données à des fins de ciblage directement sur Facebook, voir: https://newsroom.fb.com/news/h/shutting-down-partner-categories/ (consulté le 04.01.2019).

[142] ANDREOU ET AL., p. 5.

[143] LinkedIn Audience Network: https://business.linkedin.com/fr-fr/marketing-solutions/native-advertising/linkedin-audience-network (consulté le 04.04.2019) ; Facebook Audience Network: https://www.facebook.com/business/help/788333711222886 (consulté le 04.04.2019).

[144] Facebook, *A propos du processus de vérification des applications, sites web ou Pages Facebook où vos publicités peuvent apparaître,* disponible sur: https://www.facebook.com/business/help/409950705796014 (consulté le 04.04.2019). Pour la liste d'éditeurs sélectionnés par Facebook: https://www.facebook.com/block_lists/publisherlist?act=257529201612344&nav_source=mega_menu.

[145] Cette définition correspond à celle de l'art. 3 let. a LPD selon laquelle sont des données personnelles « toutes les informations qui se rapportent à une personne identifiée ou identifiable ». Par contre, contrairement au RGPD, l'art. 3 let. b LPD étend la notion de données personnelles aux données concernant les personnes morales. La version révisée de la LPD (ci-après: P-LPD) prévoit de limiter cette notion aux personnes physiques uniquement.

Cette condition est réalisée « lorsque, en raison de son contenu, sa finalité ou son effet, l'information est liée à une personne déterminée »[146]. Dans le cas du profilage, l'élément pertinent est celui de « finalité », selon lequel une information *concerne* une certaine personne lorsque les données sont utilisées afin d'influer ou d'évaluer son comportement[147]. Précisons encore que tout type de données est concerné par cette notion, comme une image, un texte, un son, un chiffre, un signe ou la combinaison de tels éléments[148]. La personne concernée doit être identifiée ou identifiable, c'est-à-dire que l'information doit se rapporter à la personne concernée directement ou indirectement par un recoupement par exemple[149] ou « par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, psychologique (…) »[150].

Une personne est identifiée lorsque son identité découle directement de l'information elle-même[151]. L'*identifiabilité* fait référence au moment où, combiné à d'autres informations, il est possible d'attribuer une information à une personne[152]. Ainsi, le caractère identifiable ne doit pas nécessairement établir l'identité civile de la personne concernée, mais doit simplement permettre de la distinguer d'autres individus[153]. Une personne est en outre identifiable lorsque son identité peut être déduite de la corrélation de plusieurs éléments d'information, grâce à des moyens technologiques[154]. Avec les nouvelles technologies et techniques algorithmiques d'analyse des données, il est plus aisé de combiner les données collectées et de les attribuer à une personne déterminée, même si ces données sont initialement anonymes ou anonymisées[155].

[146] CJUE, Arrêt C-434/16 du 20 décembre 2017, points 34-35 (affaire Novak). Dans le même sens: JAHNEL/BERGAUER, in TK DS-GVO, art. 4 N 12 ; GR29, WP136, p. 10.
[147] GR29, WP136, p. 11.
[148] KLAR/KÜHLING, in: DS-GVO Kommentar, art. 4 N 8-9 ; JAHNEL/BERGAUER, in TK DS-GVO, art. 4 N 9-11.
[149] BEELEN, p. 19.
[150] Art. 4 point 1) RGPD.
[151] KLAR/KÜHLING, in: DS-GVO Kommentar, art. 4 N 18. *Cf.* aussi: CJUE, Arrêt C-582/14 du 19 octobre 2016, point 38 (affaire Breyer).
[152] KLAR/KÜHLING, in: DS-GVO Kommentar, art. 4 N 19.
[153] SARGSYAN, p. 82 ; DE TERWANGNE, in: *Le Règlement général sur la protection des données*, p. 64.
[154] BEAT, in: HK DSG, art. 3 N 10 ss ; MEIER, p. 202.
[155] BEAT, in: HK DSG, art 3 N 15. *Cf.* aussi: ATF 138 II 346 consid. 6.1.

Dans le même sens, le consid. n° 30 RGPD précise que les identifiants en ligne tels que les adresses IP[156] et les cookies[157], qui sont attribués à une personne, sont des données à caractère personnel, puisque les personnes concernées sont potentiellement identifiables[158].

B. Application aux traitements de données à des fins de ciblage publicitaire

Dans la mesure où il n'est pas nécessaire d'établir l'identité civile de la personne, mais de la possibilité de l'identifier parmi d'autres, la législation relative à la protection des données couvre le profilage effectué par les différentes techniques de collecte de données et de suivi en ligne. Une personne est identifiable lorsque, par corrélation indirecte d'informations, on peut l'identifier. En relation avec le profilage, l'*identifiabilité* indirecte a une certaine importance[159]. Néanmoins, le traitement de données sur la base d'un profilage n'implique pas automatiquement le traitement de données *à caractère personnel,* car le traitement peut initialement reposer sur des données anonymes ou anonymisées. Si la constitution de profils sur la base de données « livrées » par les utilisateurs concernés (*profilage spécifique*) est un traitement de données à caractère personnel[160], il n'en va pas aussi clairement des données récoltées à la suite d'un *profilage abstrait* par l'observation de comportements ou d'actions. Ainsi, en tenant compte uniquement de l'observation en ligne et de la collecte, les données anonymes ou non encore attribuées à un profil n'entrent pas, à ce stade du processus, dans la définition de données à caractère personnel. Si l'on suit ce raisonnement, la législation sur la protection des données ne serait applicable qu'à partir du moment où les données sont attribuées à un profil-utilisateur ou à partir du moment où la combinaison d'une quantité suffisante de données permet de les rattacher à un profil-utilisateur et donc à une personne identifiable[162].

---

[156] À titre d'exemple, le Tribunal fédéral a considéré que l'adresse IP est une donnée personnelle qui identifie la personne au travers de la machine qu'elle utilise ; ATF 136 II 508 - 1C_285/2009 du 8 septembre 2010 (Affaire Logistep). Il en fût de même pour la CJUE dans plusieurs affaires: C-70/10 du 24 novembre 2011 (affaire Scarlet Extended), C-582/14 du 19 octobre 2016 (affaire Breyer). Dans l'affaire Breyer, la Cour a considéré que l'adresse IP dynamique était une donnée à caractère personnel dans certaines circonstances. La Cour a retenu que bien que l'adresse IP dynamique ne permette pas d'identifier directement un utilisateur, ce dernier pouvait néanmoins indirectement être identifié par la combinaison de son adresse IP à d'autres données détenues par le fournisseur d'accès internet. La Cour s'est prononcée sur la question de savoir si, pour déterminer si une personne est identifiable, il convient de se fonder sur le critère « objectif » ou le critère « relatif ». Selon l'identifiabilité objective, une adresse IP est une donnée personnelle pour tout exploitant qui en a la possession, car le FAI a la possibilité de la relier à d'autres éléments et ainsi identifier l'utilisateur. Selon l'identifiabilité relative, l'adresse IP est une donnée personnelle uniquement du point de vue du FAI puisqu'aucune autre personne n'a la possibilité d'identifier l'utilisateur, ni ne peut accéder aux données détenues par le FAI, à moins de disposer d'un moyen légal d'accéder aux informations détenues par le FAI. La Cour semble avoir adopté le critère « relatif » en considérant qu'une information qui n'identifie pas directement une personne doit être qualifiée de donnée personnelle lorsque la partie qui la possède peut légalement obtenir auprès d'un tiers (par exemple le FAI) d'autres informations permettant de la relier à l'identité d'une personne.

[157] Les données des cookies sont considérées comme étant des données personnelles du moment où elles permettent de recueillir des données d'identification tel que l'adresse IP ou du moment où les données peuvent être attribuées à des caractéristiques d'identification de l'utilisateur ou à un profil-utilisateur ; PASSADELIS/ROSENTHAL/THÜR, p. 686 ss. Il en va de même pour les *device fingerprinting*: KLAR/KÜHLING, in: DS-GVO Kommentar, art. 4 N 36.

[158] KLAR/KÜHLING, in: DS-GVO Kommentar, art. 4 N 36.

[159] WALTER, p. 98.

[160] *Idem*, p. 99.

[162] GR29, WP136, p. 14. Dans le même sens, certains auteurs énoncent que lorsque l'analyse porte sur un ensemble important de données anonymes, il reste possible de les relier à un individu déterminé, de sorte que ces données sont à qualifier de données à caractère personnel ; KING/FORDER, pp. 703-704.

MEIER stipule à raison que lorsqu'un profil abstrait est attribué à une personne déterminée, « il s'individualise ou se concrétise », ce qui rend la législation relative à la protection des données applicable à son sujet[163]. Cela sera d'autant plus le cas lorsque ces données anonymes sont combinées ou susceptibles d'être combinées à des informations « connues », telles que celles livrées directement par la personne concernée. Ces combinaisons de données anonymes se regroupent avec d'autres données personnelles ou non et permettent d'établir des profils de personnes identifiables.

S'agissant des réseaux sociaux, nous pouvons nous interroger sur la question de savoir si la personne concernée n'est réellement identifiable qu'en cours de processus, c'est-à-dire après avoir regrouper les données anonymes ou anonymisées avec les données connues de la personne concernée. Ou si, au contraire, une attribution de ces données au profil-utilisateur a lieu simultanément à la collecte, étant donné qu'il ne paraît pas impossible de faire instantanément correspondre les données collectées à son identifiant social. Dans ce cas là, la personne faisant l'objet du suivi en ligne est identifiable dès les premières étapes du profilage. À plus forte raison, les réseaux sociaux emploient des techniques de suivi en ligne non seulement dans le but de déterminer les centres d'intérêt, préférences et habitudes des internautes mais également, et surtout, dans le but de les identifier. Il importe peu à l'annonceur et au réseau social de connaître l'identité civile de la personne concernée[164], ce qui compte c'est que la personne qui se voit afficher une publicité ait été préalablement identifiée comme étant susceptible d'y réagir. Le consid. n° 26 RGPD ajoute que « Pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés (…) pour identifier la personne physique directement ou indirectement, tel que le ciblage. ». En recourant aux techniques de profilage, les données « classiques » d'identification telles que le nom et l'âge ne sont pas absolument nécessaires pour distinguer une personne. La seule probabilité d'identifier les personnes concernées en mettant les informations collectées en relation avec un identifiant suffit à entraîner l'application de la législation sur la protection des données[165]. En ce qui concerne les réseaux sociaux, les données collectées à la suite de l'observation et du suivi de leurs comportements et actions en ligne sont reliées avec leur identifiant d'utilisateur, ce qui rend leur identification possible[166].

En somme, quand bien même les premières étapes d'un profilage abstrait traitent de données anonymes ou anonymisées, les données sont à qualifier de données à caractère personnel concernant une personne identifiable à partir d'un moment donné ou d'une certaine quantité de données traitées. Une partie de la doctrine est sur ce dernier point d'avis que malgré le caractère initialement anonyme des données, la législation sur la protection des données devrait évoluer et prendre en considération l'existence des quantités importantes de données disponibles sur Internet qui rendent possible l'association d'un internaute à un profil précis[167]. Pour ce qui est du ciblage, les profils sont déjà constitués et les personnes sont par conséquent identifiées, de sorte qu'à ce stade du processus, les données traitées sont des données à caractère personnel d'une personne identifiable ou identifiée.

[163] MEIER, p. 226. Pour un raisonnement similaire: KING/FORDER, pp. 703-704.
[164] SARGSYAN, p. 84.
[165] GR29, WP171, pp. 8-9.
[166] SARGSYAN, p. 84.
[167] TUFFÉRY, *La science des données,* p. 32 ; WALTER, p. 108.

CHAPITRE 2: LICÉITÉ DU TRAITEMENT DE DONNÉES À DES FINS DE CIBLAGE PUBLICITAIRE

A. Quelques principes généraux

Les principes de base relatifs à la protection des données sont énoncés à l'art. 5 RGPD. Il s'agit des principes de licéité (art. 5 par. 1 point a) RGPD), de loyauté et de transparence (art. 5 par. 1 point a) RGPD), de limitation des finalités (art. 5 par. 1 point b) RGPD), de minimisation des données (art. 5 par. 1 point c) RGPD), d'exactitude (art. 5 par. 1 point d) RGPD), de limitation de la conservation (art. 5 par. 1 point e) RGPD), d'intégrité et de confidentialité (art. 5 par. 1 point f) RGPD) et de responsabilité (art. 5 par. 2 RGPD). Ainsi, pour être admissibles, les traitements de données doivent respecter chacun de ces principes. Pour la présente contribution, seuls les principes semblant être les plus pertinents en matière de traitement de données à des fins de publicités ciblées seront présentés, à savoir les principes de transparence (ch. 1), de limitation des finalités (ch. 2) et de minimisation des données (ch. 3).

1. Principe de transparence

Au vu du caractère invisible du profilage pour la personne concernée, le principe de transparence[168] prévu à l'art. 5 par. 1 point a) RGPD est d'une importance particulière[169]. Ce principe implique que le responsable du traitement doit, selon l'art. 12 par. 1 RGPD, fournir toutes informations sur le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples. Ce devoir d'information existe indépendamment de la nature des données traitées[170]. Les personnes concernées devraient recevoir des informations claires et simples sur la manière dont les données sont collectées, en faisant notamment référence au profilage, aux différentes techniques d'observation et de suivi tant à l'interne qu'à l'externe de la plate-forme[171], comment elles sont utilisées et pour quelles finalités, pour lesquelles elles sont utilisées comme la collecte d'informations sur les sites web visités, les interactions avec des contenus ou de la publicité[172].

Lorsque le responsable du traitement prend des décisions exclusivement automatisées, y compris le profilage, au sens de l'art. 22 par. 1, RGPD, il doit en outre informer la personne concernée de l'existence d'un tel traitement, de la logique sous-jacente, de l'importance et des conséquences pour cette dernière[173].

---

[168] Le principe de la transparence n'est pas inscrit expressément en tant que tel dans la LPD mais découle du principe de reconnaissabilité prévu à l'art. 4 al. 4 LPD ; MEIER, p. 274 ss ; HK-ROSENTHAL, art. 4 N 51-65.

[169] Le consid. n° 58 RGPD dispose sur ce point que « Le principe de transparence vaut (…) tout particulièrement dans des situations où (…) la complexité des technologies utilisées font en sorte qu'il est difficile pour la personne concernée de savoir et de comprendre si des données à caractère personnel la concernant sont collectées, par qui et à quelle fin, comme dans le cas de la publicité ciblée en ligne. ».

[170] Contrairement à l'art. 4 al. 4 LPD qui limite le devoir d'information lors de la collecte et du traitement de données sensibles et de profils de la personnalité. Dans les autres cas, la collecte de données et les finalités du traitement doivent être reconnaissables pour la personne concernée (principe de reconnaissabilité). Néanmoins, lorsque le traitement de données n'est pas reconnaissable par les personnes concernées, il est nécessaire de fournir une information active. *Cf.:* MAURER-LAMBROU/STEINER, in: BSK DSG/BGO, art. 4 N 16a ss ; MEIER, p. 274 ss ; BAERISWYL, in HK DSG, art. 4 N 47 ss.

[171] GR29, WP171, p. 21.

[172] SARGSYAN, pp. 98-99 ; GR29, WP171, p. 18.

[173] Art. 13 par. 2 point f) et art. 14 par. 2 point g) RGPD. Le projet de révision de la LPD prévoit à son art. 19 un système légèrement différent du RGPD. Contrairement à l'art. 22 RGPD qui prévoit un régime d'interdiction sous réserve d'exception, l'art. 19 P-LPD prévoit uniquement un devoir d'information en cas de décision exclusivement

Une difficulté à assurer le respect de cette obligation existe en particulier à l'égard des traitements qui recourent à de puissants outils algorithmiques et à des mécanismes complexes tels que le *data mining*. À ce sujet, le GR29 précise qu'il ne doit pas s'agir d'une explication complexe des algorithmes utilisés, ni même de leur divulgation[174]. Il suffit que les personnes concernées puissent au moins comprendre les raisons de la décision ou les critères sur lesquels elle est fondée[175]. Précisons que nonobstant un devoir d'information accru prévu aux art. 13 par. 2 point f) et 14 par. 2 point g), RGPD, le consid. n° 60 RGPD prévoit un devoir d'information légèrement renforcé pour tous les cas de profilage. Le responsable du traitement doit en outre informer la personne concernée de l'existence d'un profilage et les conséquences de celui-ci[176].

Ajoutons qu'avertir de manière générale que des traitements de données « à des fins de marketing » ont lieu ne constitue pas une information suffisante pour considérer que les utilisateurs sont informés de manière claire et compréhensible sur l'existence d'un traitement, sa mise en œuvre et ses finalités. Les utilisateurs n'ont alors pas suffisamment conscience ni ne comprennent l'ampleur des traitements mis en place. S'agissant de la manière dont l'information devrait être livrée sur Internet, le GR29 considère qu'elle devrait à tout le moins être fournie directement sur l'écran, de manière interactive, visible et compréhensible pour être conforme au principe de transparence et au devoir d'information[177]. Ainsi, l'obligation d'information peut être satisfaite par le biais d'un lien hypertexte contenant des informations relatives à l'utilisation des données des utilisateurs membres de la plate-forme, à condition d'être visible, accessible et compréhensible pour l'utilisateur.

2. Principe de finalité

Le principe de limitation des finalités, prévu à l'art. 5 par. 1 point b) RGPD, comporte deux éléments[178]. Le premier élément renvoi à la spécificité de la finalité, qui implique que cette dernière doit être communiquée à l'utilisateur en étant déterminée, spécifique, explicite et légitime[179]. Mentionner une finalité de manière générale, comme l'amélioration de l'expérience-utilisateur ou la personnalisation des publicités, ne suffit pas pour satisfaire au respect de ce principe[180]. Le second élément du principe de limitation des finalités est l'exigence d'utiliser les données collectées de manière compatible avec les buts déterminés[181]. Toutefois, cette exigence n'implique pas que les finalités du traitement de données soient parfaitement identiques à celles déclarées à l'utilisateur et pour lesquelles il a consenti[182].

---

automatisée, y compris le profilage. Le responsable du traitement devra informer de l'existence et de la logique sous-jacente mais pas de l'importance ni des conséquences du traitement (art. 19 et art. 23 al. 2 let f P-LPD).

[174] Une divulgation serait notamment incompatible avec le secret d'affaires et la propriété intellectuelle. Une telle protection est prévue au consid. n° 63 RGPD. De plus, il n'est pas certain qu'une explication aussi complexe parvienne à satisfaire au devoir d'information de façon claire et compréhensible.

[175] GR29, WP171, pp. 28-29.

[176] Consid. n° 60 RGPD.

[177] GR29, WP171, p. 21. Le consid. n° 60 du RGPG stipule en outre que la délivrance d'informations sous forme de symboles, d'images ou de pictogrammes devrait être autorisée dès lors qu'elle permet d'apercevoir de manière significative les traitements prévus sous une forme facilement perceptible et compréhensible.

[178]: SARGSYAN, p. 101.

[179] *Ibid*. Dans le même sens: DE TERWANGNE, in: *Le Règlement général sur la protection des données*, pp. 94-98.

[180] *Ibid.*

[181] Art. 5 par. 1 point b) RGPD. *Cf.*: SARGSYAN, p. 102.

[182] SARGSYAN, p. 102. *Cf.* aussi: GR29, WP203, p. 21.

Il suffit que les finalités pour lesquelles le traitement est effectivement effectué soient compatibles avec celles auxquelles l'utilisateur a consenti[183]. Un des critères pour déterminer la compatibilité des finalités déclarées avec les finalités effectives, également précisé à l'art. 6 par. 4, RGPD, est l'attente raisonnable de la personne concernée. En d'autres termes, savoir si la personne concernée pouvait ou pas raisonnablement s'attendre à ce que ses données soient traitées pour une telle finalité permet d'admettre que des données soient traitées pour une finalité certes pas identique à ce qui a été initialement déclaré à la personne concernée mais à tout le moins compatible[184]. Cela pourrait notamment être le cas pour les activités de profilage à des fins de publicités ciblées[185].

3. Principe de minimisation des données

Expression du principe de la proportionnalité[186], le principe de minimisation[187] des données exige que les données soient adéquates, pertinentes et limitées au strict nécessaire au regard des finalités envisagées[188]. La nécessité s'analyse au regard tant de la quantité que de la qualité des données[189]. Le choix du mode traitement, l'étendue et la nature des données sont autant d'éléments à limiter dans la mesure du possible afin de respecter ce principe[190].

À l'heure actuelle du Big Data et de la collecte massive de données, satisfaire ces exigences peut s'avérer complexe, d'autant plus que les technologies ne peuvent qu'encourager les entreprises à collecter plus de données que ce dont elles ont réellement besoin[191]. Les exploitants des réseaux sociaux devraient ainsi s'interroger sur le caractère adéquat, pertinent et nécessaire des quantités de données traitées à des fins de ciblage publicitaire. Nous pouvons raisonnablement douter de la nécessité de la collecte et du traitement de l'énorme quantité de données traitées par les exploitants pour parvenir à une publicité personnalisée, notamment au vu de la diversité des informations recueillies et de leurs sources. Néanmoins, la finalité « réelle » du traitement de données à des fins publicitaires va au-delà d'un ciblage précis et efficace. L'objectif poursuivi par l'exploitant, par le biais des services publicitaires, n'est d'autre que de générer du revenu. Cet aspect fera l'objet d'une analyse approfondie au moment de traiter la question de la nécessité à l'exécution du contrat (Partie 2, Ch. 2, B, ch. 2).

---

[183] GR29*,* WP203, p. 3: *Cf.* aussi: THOUVENIN, pp. 72-73. Pour davantage de précision quant au critère de « compatibilité », voir: SARGSYAN, p. 102 ; GR19, WP203, pp. 3 et 10. ; *idem,* pp. 23-27

[184] SARGSYAN, p. 102. *Cf.* aussi: GR29, WP203, pp. 3 et 10 ; *idem,* pp. 23-27.

[185] *Ibid.*

[186] En droit suisse, l'art. 4 al. 2 LPD prévoit que le « traitement doit être effectué conformément aux principes de la bonne foi et de la proportionnalité. ». La conséquence de ce principe en matière de protection des données est que seules les données aptes et objectivement nécessaires pour atteindre le but visé peuvent être traitées. Lorsque le traitement de données a lieu dans l'intérêt de la personne concernée, le principe de la proportionnalité n'a pas la même portée que lorsque le traitement est dans l'intérêt du responsable du traitement ou d'un tiers. A propos du principe de la proportionnalité, voir MAURER-LAMBROU/STEINER, in: BSK DSG/BGO, art. 4 N 9 ss ; MEIER, p. 267 ss ; BAERISWYL, in HK DSG, art. 4 N 20 ss ; HK-ROSENTHAL, art. 4 N 19 ss.

[187] Art. 5 par. 1 point c) RGPD.

[188] DE TERWANGNE, in: *Le Règlement général sur la protection des données,* p. 107-108.

[189] *Idem,* p. 108.

[190] MEIER*,* p. 271.

[191] GR29, WP251 rév.01*,* p. 12.

B. Justification du traitement

Le RGPD exige l'existence d'une base juridique au traitement pour que celui-ci puisse valablement avoir lieu (principe de l'interdiction sous réserve d'autorisation), indépendamment de l'existence d'une atteinte à la personnalité ou de la violation d'un ou de plusieurs principes relatifs à la protection des données[192].

Ainsi, l'art. 6 RGPD liste les hypothèses dans lesquels un traitement de données à caractère personnel est licite. Le seul respect d'un de ces motifs rend le traitement de données à caractère personnel licite, sans toutefois exonérer le responsable du traitement du respect des principes figurant à l'art. 5 RGPD. Ces hypothèses sont au nombre de six, à savoir le consentement, le contrat, l'obligation légale, la sauvegarde d'un intérêt vital, la mission d'intérêt public ou relevant de l'exercice de l'autorité publique et enfin les intérêts légitimes du responsable du traitement ou d'un tiers[193].

Pour la présente contribution seront pertinents le consentement de l'utilisateur (ch. 1), la nécessité à l'exécution du contrat d'utilisation entre l'exploitant du réseau social et l'utilisateur (ch. 2) et l'intérêt légitime du responsable de traitement ou d'un tiers (ch. 3).

1. Consentement de l'utilisateur

Le consentement se définit comme « toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement »[194]. En d'autres termes, le consentement est l'expression d'une intention volontaire, en connaissance de cause, sans ambiguïté et donné par une déclaration ou tout autre acte d'acceptation sans équivoque[195].

On peut admettre qu'un consentement est donné lorsqu'une personne accepte des conditions d'utilisation sans en avoir pris effectivement connaissance, mais qu'elles lui étaient disponibles et raisonnablement accessibles avant la conclusion du contrat[196]. Il est utile de préciser sur ce point que les réseaux sociaux mettent à disposition des utilisateurs des explications sur la manière dont leurs données sont utilisées et à quelles fins.

---

[192] Contrairement au RGPD, l'art. 13 al. 1 LPD énumère les motifs justificatifs qui justifient un traitement de données portant atteinte à la personnalité. Tel est notamment le cas en cas de violation d'un ou de plusieurs principes ou en cas de traitement de données contraire à la volonté expresse de la personne concernée. Le P-LPD prévoit en plus, en tant qu'atteinte à la personnalité, le profilage sans le consentement exprès de la personne concernée. On compte parmi les motifs justificatif le consentement, l'intérêt prépondérant privé ou public ou la loi. Un motif justificatif n'a lieu d'être invoqué qu'en cas d'atteinte à la personnalité. Un traitement de données personnelles respectueux de toutes les exigences légales en matière de protection des données, et de surcroît qui n'attente pas à la personnalité de la personne concernée, ne doit pas nécessairement être fondé sur un motif justificatif pour pouvoir être effectué ; MEIER, p. 529 ss ; WEMELINGER, in HK DSG, art. 13 N 1 ss ; RAMPINI, in: BSK DSG/BGO, art. 13 N 1 ss.

[193] Art. 6 par. 1 points a) à f) RGPD.

[194] Art. 4 point 11) RGPD. Le droit suisse prévoit à l'art. 4 al. 5 LPD que pour être valable, le consentement doit avoir été donné librement par la personne concernée après avoir été dûment informée. Ainsi, le droit communautaire paraît plus spécifique s'agissant des conditions de validité du consentement.

[195] SÖBBING, pp. 184-185.

[196] MEIER, p. 336-337.

Sans exhaustivité et dans le but d'une meilleure analyse des conditions relatives au consentement, nous aborderons brièvement le contenu des politiques d'utilisation de plusieurs réseaux sociaux relatif au traitement de données des utilisateurs à des fins de ciblage publicitaire.

1.1 Politiques d'utilisation et contenu relatif au traitement de données à des fins de ciblage publicitaire

Pour satisfaire à la condition du consentement, l'utilisateur doit avoir accès aux politiques d'utilisation des données avant de consentir[197]. Dès lors, les politiques d'utilisation des données dont il est fait référence dans le présent chapitre ont été consultées lors d'une inscription fictive, avant de les avoir acceptées. Précisons encore que les politiques de la plupart des réseaux sociaux ont été mises à jour simultanément ou peu après la date à partir de laquelle le RGPD est devenu applicable[198]. Il est de plus utile de relever que lorsque l'utilisateur s'inscrit sur une plate-forme sociale, il octroie à cette dernière une licence non exclusive, transférable, gratuite et mondiale pour héberger et utiliser tout contenu partagé, publié ou téléchargé[199]. L'octroi de cette licence figure parmi les obligations contractuelles des utilisateurs.

Les politiques d'utilisation indiquent clairement que les données des utilisateurs sont traitées afin de fournir des contenus personnalisés, y compris de la publicité ciblée. Font ainsi l'objet de traitements les informations fournies par l'utilisateur, les activités à l'interne et à l'externe de la plate-forme, les informations du dispositif telles que l'adresse IP, l'identifiant et le système d'exploitation. Des informations sur la manière dont les services sont utilisés, comme les contenus consultés, les fonctionnalités utilisées, l'heure et la fréquence des activités, les informations que d'autres personnes fournissent sur l'utilisateur, la connexion Wi-Fi et les informations dont l'utilisateur a autorisé l'accès par le biais des paramètres du dispositif comme la localisation GPS ou l'appareil photo[200], sont aussi recueillies.

Tout contenu, que ce soit sous forme de textes, de vidéos ou de photos téléchargés par les utilisateurs, est traité par le réseau social. Les politiques de confidentialité de Twitter indiquent, à la différence de celles de Facebook et Instagram, que les données sont utilisées pour déduire les thèmes susceptibles d'intéresser l'utilisateur, son âge, sa langue et personnaliser le contenu, y compris les publicités. Des données en provenance d'outils intégrés à des applications ou sites web de tiers, tels que les cookies ou autres technologies similaires comme les pixels et les plugins, sont aussi recueillies. Les politiques prévoient à cet égard des explications quant à leur mécanisme, les données qu'ils permettent de collecter, les finalités et les endroits où ces outils sont intégrés[201].

---

[197] LEONARD, p. 17.

[198] Les politiques d'utilisation des données Facebook et Instagram ont été mises à jour le 19 avril 2018, celles de Twitter le 25 mai 2018.

[199] Politique d'utilisation des données Facebook, disponible sur: https://www.facebook.com/about/privacy/update (consulté le 06.04.2019) ; Conditions d'utilisation Twitter, disponible sur: https://twitter.com/fr/tos (consulté le 06.04.2919). Pour davantage d'informations quant à la signification de cette licence, voir: WAUTERS/LIEVENS/WALCKE, p. 266 et ANTREASYAN, pp. 65-67.

[200] Politique d'utilisation des données Facebook, disponible sur: https://www.facebook.com/about/privacy/update (consulté le 06.04.2019) ; Politique de confidentialité de Twitter, disponible sur: https://twitter.com/fr/privacy (consulté le 06.04.2919).

[201] Cookies et autres technologies de stockage Facebook, disponible sur: *https://www.facebook.com/policies/cookies/* (consulté le 06.04.2019) ; Notre utilisation des cookies et autres technologies similaires Twitter, disponible sur: https://help.twitter.com/fr/rules-and-policies/twitter-cookies (consulté le 06.04.2019).

Il est précisé que ces informations peuvent comprendre le type de dispositif, les sites web consultés, les achats effectués ou encore les interactions avec les publicités[202]. Nous remarquons une nette progression quant à la qualité des informations fournies dans les politiques des réseaux sociaux depuis leur mise à jour. Les utilisateurs semblent disposer des informations nécessaires pour comprendre dans les grandes lignes les mécanismes de la publicité ciblée et sur quel type de données elle se fonde. Nous constatons par ailleurs que chaque clic, chaque interaction avec le réseau social, ses services et ses applications ou avec d'autres utilisateurs sont couverts par les déclarations d'utilisation des données. Le devoir d'information paraît relativement bien mis en œuvre, mais l'est-il suffisamment ? La réponse à cette question est traitée lors de l'analyse du consentement éclairé (*infra* Partie 2, Ch. 2, B, ch. 1.2.1).

1.2 Conditions de validité du consentement

Les conditions du consentement ont été renforcées par rapport à la Directive 95/46/CE[203]. Pour être valable, celui-ci doit être éclairé (1.2.1), libre (1.2.2) spécifique et univoque (1.2.3). Un consentement explicite est en outre requis en cas de traitements de données tombant dans le champ d'application de l'art. 22 par. 1, RGPD (1.3).

1.2.1 Consentement éclairé

Les personnes concernées doivent préalablement avoir été informées, afin d'être en mesure de décider si oui ou non elles acceptent les traitements et les finalités envisagés[204]. Cette exigence concrétise le principe de transparence et le devoir d'information[205]. Ce dernier tend à garantir que les personnes concernées expriment un consentement éclairé, en toute connaissance de cause[206] et existe indépendamment de la nature des données traitées[207].

Une partie de la doctrine évoque qu'un consentement ne peut *de facto* valablement être donné en cas de recours au *data mining*[208]. En effet, elle considère qu'il s'agit d'une technique automatique et automatisée de traitement de quantités considérables de données en provenance de nombreuses sources parfois inconnues et dont il n'est pas possible de déterminer l'objectif à l'avance, ni savoir si ou comment et quelles données vont être utilisées[209]. Le responsable du traitement ne peut lui même vraisemblablement pas donner d'explications claires sur les informations générées par les techniques d'analyse des données. Il ne serait pas non plus en mesure de savoir quelle donnée ou quelle corrélation émergera du processus[210].

---

[202] Politique d'utilisation des données Facebook, disponible sur: https://www.facebook.com/about/privacy/update (consulté le 06.04.2019) ; Politique de confidentialité de Twitter, disponible sur: https://twitter.com/fr/privacy (consulté le 06.04.2919). Etant précisé que ces informations sont collectées que l'utilisateur possède ou non un compte Facebook ou qu'il soit connecté ou non à son compte.
[203] DE TERWANGNE, in: *Le Règlement général sur la protection des données*, pp. 120-121.
[204] Art. 4 point 11) et art. 13 RGPD ; MEIER, p. 329 ; RAMPINI, in: BSK DSG/BGO, art. 13 N 4.
[205] *Supra* Partie 2, Ch. 2, A, ch. 1.
[206] GR29, WP259 rév.01, p. 15.
[207] Contrairement à l'art. 4, al. 4 LPD qui limite le devoir d'information au traitement de données sensibles et de profils de la personnalité. Dans les autres cas, la collecte et les finalités du traitement doivent être reconnaissables pour la personne concernée (principe de reconnaissabilité). *Cf.:* MAURER-LAMBROU/STEINER, in: BSK DSG/BGO, art. 4 N 16a ss ; MEIER, p. 274 ss ; BAERISWYL, in HK DSG, art. 4 N 47 ss.
[208] SCHWEIZER, *Data Mining*, pp. 108-109. Dans le même sens: CAVOUKIAN, pp. 12-13.
[209] *Ibid.*
[210] CAVOUKIAN, p. 13.

HILDEBRANDT[211] souligne que dans le cas du profilage en particulier, les personnes concernées n'ont de même pas la capacité d'anticiper les conséquences de l'application des profils dérivés des données d'autres personnes, ce qui exclut la possibilité d'un consentement éclairé[212].

Satisfaire au devoir d'information en cas de recours aux technologies de collecte massive de données et au profilage est complexe. Les exploitants de réseaux sociaux devraient, pour satisfaire à ces exigences, éviter les informations trop générales concernant le traitement de données à des fins de publicités ciblées, tout en prenant garde à ne pas introduire des termes excessivement techniques ou juridiques que les utilisateurs ne seraient pas en mesure de comprendre[213]. Une liste d'exemples vagues, démonstratifs et non exhaustifs des données concernées et des traitements effectués n'est pas suffisante pour admettre un consentement éclairé. Or, comme nous pouvons le constater, les politiques d'utilisation des données, améliorées depuis l'entrée en vigueur du RGPD, s'avèrent plus complètes et claires quant aux données traitées, la manière dont elles sont traitées et leurs finalités[214]. Certaines politiques d'utilisation invoquent également que les données collectées serviront à déduire les centres d'intérêt des utilisateurs. Autrement dit, ces derniers semblent disposer d'informations nécessaires pour avoir une vue d'ensemble des différentes sources des données et leurs finalités.

Toutefois, bien qu'une meilleure conformité à la législation sur la protection des données est à remarquer, il n'en demeure pas moins que ces politiques ne sont pas exhaustives. Évoquer de manière large que leurs comportements et attitudes à l'externe comme à l'interne de la plate-forme font l'objet d'un suivi dans le but d'offrir de la publicité personnalisée n'est pas suffisant pour comprendre avec exactitude quelles données font l'objet du suivi, leurs sources exactes, la manière dont les corrélations sont faites, ni quelles données servent à ces corrélations ou quelles informations sont ensuite inférées à leur profil-utilisateur[215]. L'existence d'un profilage ne semble pas non plus être évoquée en tant que telle. Seule une infime partie des fonctionnalités et mécanismes est présentée aux utilisateurs. Par conséquent, de par leur manque d'exhaustivité et leur caractère encore trop général à notre sens, le consentement n'est pas éclairé. Nous ne sommes en revanche pas certain qu'un consentement ne puisse jamais valablement être donné comme le suggèrent certains auteurs[216]. À notre sens, cela devrait être possible puisqu'admettre le contraire viderait le consentement de tout son sens. Ces considérations méritent toutefois réflexion et sont sujettes à débat.

---

[211] HILDEBRANDT, *Who is Profiling Who*, p. 243.

[212] Certains auteurs parlent de « piège de l'autonomie » en argumentant cela par le fait que les *profilers* manipulent ou peuvent facilement manipuler une personne dans ses choix, ses actions et ses comportements en raison du fait qu'elle n'est pas consciente de ce qu'elle sait d'elle-même, ni consciente de ce qui est connu à propos de ses habitudes, par qui ces informations sont exploitées, à qui elles sont vendues, distribuées ou mises à disposition, de la manière dont elles sont utilisées pour influencer son comportement. Ceci avec pour conséquence une diminution conséquente de la capacité d'agir sur la base d'un consentement éclairé. *Cf*. aussi: HILDEBRANDT, *Who is Profiling Who*, pp. 243-244 ; ZARSKY, pp. 35-38. SCHWEIZER stipule, dans le même sens, que le *data mining* permet aux entreprises de manipuler les clients dans leur liberté de décision ; SCHWEIZER, *Data Mining,* p. 111.

[213] SARGSYAN, p. 98. *Cf.* aussi: GR29, WP259 rév.01, p. 16.

[214] *Contra* mais remontent avant les améliorations apportées à la suite du RGPD: GR29, WP171, pp. 14-15 ; KIRSCH, p. 3 ; ZUIDERVEEN BORGESIUS*,* pp. 104-105.

[215] *Cf.:* ESTEVE, p. 39 ; Formation restreinte de la CNIL, Délibération n° SAN-2017-006 du 27 avril 2017 prononçant une sanction pécuniaire à l'encontre des sociétés Facebook Inc. et Facebook Ireland. Dans ladite délibération, la CNIL a notamment considéré que « l'information dispensée via le bandeau d'information relatif aux cookies est imprécise. (…) cette mention ne fait qu'indiquer que des informations sont collectées (…) ce qui ne permet pas aux internautes d'être clairement informés et de comprendre que leurs données sont systématiquement collectées dès lors qu'ils naviguent sur un site tiers (…). »

[216] SCHWEIZER, *Data* Mining, pp. 108-109 ; CAVOUKIAN, pp. 12-13.

1.2.2 Consentement libre

Le consentement doit avoir été librement donné[217]. D'après BUCHNER, le caractère volontaire du consentement ne devrait être un élément probant que lorsque l'utilisateur dépend effectivement desdits services et qu'aucune alternative n'est envisageable[218]. Or, les modèles d'entreprises « à prendre ou à laisser » par lesquels on ne peut pas devenir membre d'un réseau social si on ne consent pas à tout pourraient *a priori* constituer une violation du caractère libre du consentement. L'absence de liberté ne se pose toutefois pas uniquement parce qu'un service est subordonné au consentement[219]. Une situation de contrainte n'existe que si aucune alternative ne se présente à l'utilisateur, y compris la possibilité de ne pas recourir du tout à un service[220]. Dès lors, le consentement au contrat d'adhésion d'un réseau social est libre compte tenu de la possibilité de ne pas recourir à ces services. La personne concernée dispose d'une véritable liberté de décision, elle a le choix de confirmer son inscription ou d'y renoncer[221]. La question est alors de savoir si cette liberté englobe également le traitement de données à des fins de ciblage publicitaire.

À notre sens, bien qu'une liberté de consentir puisse raisonnablement être admise au moment de l'inscription, celle-ci ne doit pas être rapportée au traitement de données à des fins publicitaires. Les utilisateurs n'ont pas la possibilité de donner ou de retirer librement un consentement distinct pour le traitement de données pour cette finalité, de sorte que le consentement aux politiques d'utilisation obtenu par l'exploitant du réseau social au moment de l'inscription ne saurait raisonnablement être considéré comme librement donné[222]. D'autant plus que le consentement au traitement de données à des fins commerciales est, en général, une condition *sine qua non* de la mise à disposition de la plate-forme aux utilisateurs[223], dont le seul choix est de refuser d'utiliser les services du réseau social ou d'en accepter l'ensemble des conditions d'utilisation. Toutefois, une fois inscrits, les membres de la communauté peuvent consulter et modifier leurs paramètres publicitaires. Ils ont entre autres la possibilité d'exclure certains traitements de données ou certaines catégories de données ou encore de modifier les intérêts qui leur sont assignés dans leur profil. Ces informations sont à portée des utilisateurs non pas au moment de leur inscription mais plus tard, lorsqu'ils accèdent à leurs paramètres. Encore faut-il qu'ils aient conscience que de telles informations existent pour en prendre connaissance. Le fait que ces paramètres soient accessibles *a posteriori* et nécessitent une action volontaire ne permet pas de considérer que le consentement est valable pour autant. De plus, une distinction importante est à opérer entre le profil du compte-utilisateur consultable par ce dernier et le profil créé par l'exploitant et enrichi par toutes nouvelles informations résultant de la collecte des données et du profilage. Malgré les possibilités mises à disposition des utilisateurs pour maîtriser l'affichage des annonces et, par conséquent, d'exercer leur droit à l'autodétermination en matière de publicités, cela ne suffit pas à admettre qu'un consentement est valablement donné, car les paramètres de base sont configurés de façon à ce que les publicités ciblées soient autorisées dès le départ et qu'une action de l'utilisateur soit nécessaire s'il ne souhaite pas recevoir d'annonces personnalisées[224]. Un consentement implicite ne peut non plus être déduit du défaut d'action de l'utilisateur[225].

---

[217] Art. 4 point 11) RGPD
[218] BUCHNER, p. 3.
[219] *Ibid*.
[220] *Ibid*.
[221] *Ibid*.
[222] SARGSYAN, pp. 95-96.
[223] *Idem*, p. 96. *Cf.* aussi: ANTREASYAN, pp. 61 et 136-142
[224] *Cf.* aussi: OBERLIN, *Teil 2*, p. 69.
[225] KIRSCH, pp. 11-14.

La condition du consentement libre serait réalisée si les utilisateurs avaient le choix d'accepter ou non que leurs données soient traitées à des fins de ciblage publicitaire, sans que l'accès aux services du réseau social n'en soit compromis au moment de leur inscription. Cela nous amène en conclusion à considérer, au vu des éléments exposés ci-avant, que l'exigence relative au consentement libre n'est pas réalisée en matière de publicité ciblée sur les réseaux sociaux.

1.2.2.1 Consentement nécessaire à l'exécution du contrat ou à la fourniture de services

Précisant la portée du caractère libre du consentement, le consid. n° 43 RGPD mentionne que celui-ci « est présumé ne pas avoir été donné librement (…) si l'exécution d'un contrat, y compris la prestation d'un service, est subordonnée au consentement malgré que celui-ci ne soit pas nécessaire à une telle exécution. »[226]. L'art. 7 par. 4, RGPD stipule en outre que pour « déterminer si le consentement est donné librement, il y a lieu de tenir (…) compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat ». Cela signifie qu'un consentement n'est pas librement donné si l'exécution du contrat a été subordonnée au consentement au traitement de données non nécessaire pour l'exécution dudit contrat. Cette règle énonce l'interdiction de lier le consentement à l'exécution du contrat ou à la fourniture de services qui n'est pas nécessaire[227].

L'exécution du contrat d'utilisation est généralement subordonnée au consentement au traitement de données à des fins publicitaires. La doctrine considère qu'au vu du consid. n° 43 et de l'art. 7 par. 4, RGPD, les exploitants de réseaux sociaux devraient organiser leurs services de telle sorte que le consentement au traitement des données qui n'est pas nécessaires pour l'exécution des prestations « de base », comme c'est le cas de la publicité ciblée, ne soit pas lié à tous les services confondus[228]. Ne partageant pas entièrement cet avis, nous renvoyons le lecteur au chapitre « Nécessaire à l'exécution du contrat d'utilisation » (*infra* Partie 2, Ch. 2, B, ch.2) ci-dessous qui développe plus en détails la question de la nécessité de la publicité ciblée.

1.2.3 Consentement spécifique et univoque

Le caractère spécifique du consentement tient au fait qu'il ne peut être donné *de manière général*[229] et couvrir l'ensemble des finalités envisagées par le responsable du traitement mais doit, au contraire, porter sur des traitements précisément déterminés[230]. La personne concernée devrait avoir le choix de consentir à une finalité indépendamment des autres[231]. Si le traitement de données sert plusieurs finalités, un consentement est requis pour chacune des finalités[232]. Afin d'assurer la réalisation de cette condition, il convient de distinguer chaque finalité des traitements poursuivis pour que les personnes concernées puissent consentir à chaque finalité.

---

[226] Consid. n° 43 RGPD. Critère également repris à l'art. 7 par. 4 RGPD.
[227] BUCHNER/KÜHLING, in: DS-GVO Kommentar, art. 4 Nr. 11 N 6 ; *idem,* art. 7 N 46 ss.
[228] SARGSYAN, pp. 96-97.
[229] GR29, WP259 rév.01, p. 19.
[230] LEONARD, p. 16: SARGSYAN, p. 100 ; GR29, WP187, pp. 19-21. Le droit suisse ne comporte pas d'exigence de spécificité du consentement. Néanmoins, cette condition peut être déduite des principes de proportionnalité (art. 4 al. 2 LPD), de finalité (art. 4 al. 4LPD), de reconnaissabilité (art. 4 al. 4 LPD) et du devoir d'information dans certains cas (art. 14 LPD). Voir: SARGSYAN, p. 101 ; BAERISWYL, in HK DSG, art. 4 N 20-33, N 47-53 ; WERMELINGER, in HK DSG, art. 14 N 1 ss.
[231] GR29, WP259 rév.01, p. 13.
[232] AUF DER MAUR/FEHR-BOSSHARD, p. 11.

L'utilisateur devrait avoir la possibilité de donner un consentement libre, éclairé et spécifique s'agissant du traitement de ses données à des fins de ciblage publicitaire, indépendamment de son accès à la plate-forme[233]. Toutefois, il semble que l'utilisateur n'ait pas une liberté de consentir à une finalité indépendamment de l'autre au moment de son inscription. Il paraît alors raisonnable de s'interroger sur la question de savoir si la possibilité accordée par les réseaux sociaux de modifier les paramètres publicitaires, et de ne pas recevoir de publicité personnalisée ou de restreindre le traitement à certaines catégories de données après l'inscription effectuée, suffit à satisfaire l'exigence de spécificité.

Nous sommes d'avis que la faculté de modifier ses paramètres après coup ne réalise pas l'exigence de spécificité[235]. En d'autres termes, l'utilisateur ne peut pas accepter le traitement de ses données pour assurer les services « de base » sans pour autant refuser que ses données soient traitées à des fins de ciblage publicitaire. Cette exigence n'est donc pas réalisée et le consentement des utilisateurs n'est pas spécifique s'agissant du traitement de leurs données pour de la publicité. Par ailleurs, malgré la possibilité laissée à l'utilisateur de modifier ses paramètres pour ne plus se voir afficher de la publicité personnalisée, nous doutons que le traitement de ses données cesse pour autant. En effet, s'il est communément admis que les réseaux sociaux dressent des profils d'internautes non membres, nous pouvons raisonnablement croire que des profils sont établis également lorsqu'un utilisateur décide de ne pas recevoir de publicités ciblées[236].

Le RGPD exige que le consentement soit donné par une déclaration ou un acte positif clair[237], par exemple au moyen d'une déclaration écrite ou orale ou par le fait de cocher une case sur une page Internet[238]. Il doit être évident que la personne concernée consent au traitement envisagé. Le silence, l'inaction ou les cases précochées n'expriment pas un consentement, de même que le fait pour une personne de continuer à utiliser un service[239].

Le consentement doit avoir été donné de manière à démontrer sans équivoque l'intention de la personne concernée d'accepter le traitement de ses données[240]. Il est par exemple admis que le fait que l'utilisateur coche une case « Je consens » est un acte positif clair équivalent à un consentement, y compris lorsqu'un avis de confidentialité comprenant les informations nécessaires est disponible de manière *superposée*[241]. Il apparaît que les mécanismes prévus lors de l'inscription aux réseaux sociaux, à savoir le fait pour un utilisateur de devoir cocher une case « Inscription » accompagnée de liens hypertextes contenant des informations sur le traitement de leurs données, satisfont à l'exigence d'univocité.

---

[233] GR29, WP187, p. 20.
[235] *Cf. Supra* Partie 2, Ch. 2, B, ch. 1.2.2.
[236] Lors de son audition du mois d'avril 2018 devant le Sénat américain, Mark Zuckerberg a déclaré que l'entreprise Facebook collectait des données de personnes non inscrites pour des raisons de sécurité. En ce qui concerne la collecte de données d'individus non membres d'un réseau social, *cf.* notamment: PRAZ, p. 8 pour ce qui est de la collecte d'informations d'internaute non membres par le biais des plugins sociaux.
[237] Art. 4 point 11) RGPD ; DE TERWANGNE, in: *Le Règlement général sur la protection des données*, p. 125.
[238] Consid. n° 32 RGPD.
[239] GR29, WP259 rév.01, p. 18.
[240] SARGSYAN, p. 93.
[241] Exemple tiré de GR29, WP259 rév.01, pp. 17-19.

1.3 Condition spécifique de validité: le consentement explicite

1.3.1 Champ d'application de l'article 22 RGPD

En ce qui concerne le profilage et les décisions automatisées en particulier, le RGPD a introduit des dispositions spécifiques supplémentaires[242]. Nous sommes en présence d'une prise de décision exclusivement automatisée lorsque celle-ci résulte de moyens techniques sans intervention humaine[243]. Celle-ci peut être le résultat d'un profilage ou avoir été prise sans profilage[244]. La décision peut être basée sur des données fournies par la personne concernée, des données observées, dérivées ou inférées[245]. En termes de publicités ciblées, l'annonce présentée à l'utilisateur constitue une prise de décision entièrement automatisée[246], puisqu'elle résulte d'un processus algorithmique, c'est-à-dire d'un profil produit par des moyens techniques purement automatisés. Par conséquent, si la publicité ciblée est une décision exclusivement automatisée[247], la question est de savoir si cette dernière déploie des effets juridiques ou d'effets affectant de manière significative et similaire la personne concernée au sens de l'art. 22 par. 1, RGPD[248].

Le RGPD n'indique pas ce qu'il faut entendre par « produisant des effets juridiques (…) ou l'affectant de manière significative de façon similaire ». À notre sens, l'affichage de la publicité ciblée, en tant que décision exclusivement automatisée, est susceptible d'entraîner des effets affectant l'utilisateur de manière similaire à des effets juridiques dans des cas limités, par exemple en cas de discrimination ou lorsque la publicité vise des personnes vulnérables. En reprenant un exemple du GR29[249], ce sera notamment le cas pour une personne dont il est connu qu'elle est sujette à des difficultés financières mais qui est régulièrement ciblée par des publicités pour des prêts. Si la publicité parvient à influencer cette personne, cela aura pour conséquence que cette dernière s'endettera davantage.

Si la publicité ciblée en tant que telle n'est susceptible d'entrer dans le champ d'application de l'art. 22 RGPD que dans des cas limités, il en va différemment du profilage la précédant. Sur ce point, le GR29 a adopté une approche extensive de la condition de l'art. 22 par. 1, RGPD relative aux effets qui doivent affecter de manière similaire à des effets juridiques et de façon significative la personne concernée. Le groupe considère que le profilage en matière de publicité ciblée pourrait *dans certains cas* remplir la condition prévue à l'art. 22 par. 1, RGPD, en raison des conséquences produites à l'égard des personnes exposées à cette publicité[250].

---

[242] Il s'agit en particulier des art. 13 par. 2 point f), 14 par. 2 point g) et 22 RGPD.

[243] GR29, WP251 rév.01, p. 8 ; SCHULTZ, in: Kommentar DS-GVO, art. 22 N 12 ss. *Cf.* aussi: THOUVENIN/FRÜH/GEORGE, N 4-8.

[244] GR29, WP251 rév.01, p. 9.

[245] *Ibid.*

[246] Dans le même sens: GR29, WP251 rév.01, p. 24.

[247] SARGSYAN, p. 89. Pour davantage d'explications, voir: BYGRAVE, pp. 18-19.

[248] L'art. 19 P-LPD prévoit un concept différent du RGPD puisqu'il y énonce une obligation d'information en cas de décision exclusivement automatisée et non pas une interdiction. Cette obligation s'éteint lorsque la décision est en rapport direct avec la conclusion ou l'exécution d'un contrat ou lorsque la personne concernée y a expressément consenti. Voir: THOUVENIN/FRÜH/GEORGE, N 27.

[249] GR29, WP251 rév.01, p. 24-25. BYGRAVE donne l'exemple d'une personne qui se verrait offrir des produits à un prix plus élevé qu'à d'autres ; BYGRAVE, p. 20.

[250] GR29, WP251 rév.01, p. 24. Cette position est également partagée par BYGRAVE, p. 20.

Ce sera, entre autres, le cas lorsque le profilage paraît particulièrement intrusif, y compris lors du suivi des personnes sur différents sites web, appareils et services ou lorsque le processus recourt aux vulnérabilités des personnes ciblées. À tout le moins, les effets sont de nature significative lorsqu'ils touchent à l'épanouissement personnel de la personne concernée[251].

En ce qui concerne la publicité ciblée sur les réseaux sociaux, l'appréciation du caractère intrusif du profilage est alors déterminante pour savoir si les dispositions spécifiques sont applicables ou pas. Selon nous, le caractère intrusif peut raisonnablement être admis au vu des nombreuses sources depuis lesquelles les données sont collectées et la quantité sans précédent d'informations traitées, voire de la manière dont le suivi est effectué, si celui-ci a lieu à l'insu. L'accroissement exponentiel des moyens technologiques de collecte et d'analyse des données[252] est une raison supplémentaire en faveur de la reconnaissance d'un aspect intrusif à la publicité ciblée. Ce caractère est d'autant plus à admettre au vu des possibilités, pour les annonceurs, de cibler les utilisateurs sur la base de critères relevant de catégories de données particulières et en principe prohibées, tel que les intérêts politiques ou religieux[253]. Toutefois, la question est sujette à discussion, tant il est plausible qu'un tel caractère ne soit reconnu que dans certains cas et non pas de façon systématique, ou ne soit admis qu'à partir d'un certain moment, par exemple lorsque les données récoltées vont au-delà des informations « de base » comme l'âge ou le sexe[254].

Au vu de ce qui précède et en retenant un caractère potentiellement intrusif au profilage, celui-ci est de nature à affecter de manière significative de façon similaire à des effets juridiques les utilisateurs, de sorte qu'un consentement explicite est requis.

1.3.2 Consentement explicite

L'interdiction générale d'effectuer des traitements de données entrant dans le champ d'application de l'art. 22 par. 1, RGPD peut être levée en cas de consentement explicite[255]. Le terme « explicite » fait référence à la manière dont le consentement est exprimé[256]. Ainsi, si les conditions d'un consentement « standard » exigent une déclaration ou un acte positif, la déclaration de consentement explicite doit être exprès, de manière à ce que la personne concernée comprenne la portée de son consentement[257]. Ce dernier doit en outre spécifiquement se rapporter à la partie du traitement dont un consentement explicite est nécessaire.

---

[251] BUCHNER, in: DS-GVO Kommentar, art. 22 N 26.

[252] Il est fait référence ici aux possibilités de prédire des émotions ou des états d'âmes, ce qui touche, à notre avis, l'essence même de l'être humain. Voir par exemple: KELSHAW, *Analyser les émotions,* disponible sur: https://www.thinkwithgoogle.com/intl/fr-145/industry-perspectives/articles-internationaux/analyse-de-lemotion-une-solution-efficace-pour-ameliorer-lintuition/ (consulté le 06.04.2019).

[253] *Supra* Partie 1, Ch. 2, B, ch. 5.1.

[254] Il est considéré qu'une publicité fondée sur le profilage et basée sur un simple profil démographique (âge, sexe et région) n'affecte pas la personne concernée de façon similaire et significative ; GR29, WP251 rév.01, p. 24.

[255] Art. 22 par. 2 point c) et consid. n° 71 RGPD. L'art. 4 al. 5 LPD prévoit qu'un consentement doit être explicite lorsque le traitement porte sur des données sensibles ou des profils de la personnalité. Le P-LPD entend par ailleurs remplacer la notion de profil de personnalité par celui de profilage. Sur ce point, la LPD va plus loin que le RGPD car le consentement explicite est requis en cas de profil de la personnalité, respectivement de profilage, sans qu'il soit nécessaire de démontrer que le traitement déploie des effets juridiques ou affecte de manière similaire et significative la personne concernée.

[256] GR29, WP259 rév.01, p. 21. Contrairement à la notion du RGPD, le terme explicite prévu dans la LPD se rapporte à l'objet matériel du consentement, soit à son contenu, et non pas à la façon dont la manifestation de volonté est exprimée ; MEIER, p. 343 ; HK-ROSENTHAL, art. 4 N 83. *Cf.* aussi: SARGSYAN, p. 94

[257] SCHULTZ, in: Kommentar DS-GVO, art. 22 N 32.

D'après SARGSYAN, lorsque l'utilisateur communique des informations personnelles à un réseau social, cela devrait s'interpréter comme un consentement explicite à utiliser lesdites informations[258]. Tel devrait notamment être le cas lorsque ces informations sont utilisées à des fins de bonne exécution des services de mise à disposition et d'utilisation de la plate-forme. En revanche, il n'en va pas nécessairement de même pour ce qui est de l'utilisation de ces données à des fins de publicités ciblées. Pour une telle finalité, la fourniture volontaire des informations personnelles ne devrait pas être considérée comme un consentement explicite[259]. Pour consentir à cette finalité, le responsable de traitement devrait mettre en place des mécanismes sollicitant une action positive de la personne concernée. C'est le cas lorsque l'utilisateur coche activement une case où le traitement de données soumis au consentement explicité est évoqué[260], à condition de satisfaire aux autres exigences relatives au consentement « standard ». Aussi, les réseaux sociaux offrent la plupart du temps un niveau de confidentialité par défaut. On ne saurait déduire des mécanismes d'opt-out mis en place un consentement explicite des utilisateurs[261]. L'absence d'action de l'utilisateur ne signifie par ailleurs pas qu'il consent à ce que ses données soient utilisées conformément au régime par défaut préétabli par l'exploitant de la plate-forme.

Il convient également de relever l'existence d'exigences accrues en ce qui concerne le traitement de catégories particulières de données[262]. Les exploitants de réseaux sociaux proposent parmi les critères de ciblage suggérés à l'annonceur des catégories de centres d'intérêt relevant de données sensibles, comme les opinions politiques ou religieuses[263]. La diffusion de publicité basée sur de telles données est en principe prohibée[264]. L'interdiction peut toutefois être levée sur la base d'un consentement explicite. Précisions que l'art. 9 par. 2 RGPD ne connaît pas le caractère « nécessaire à l'exécution d'un contrat » comme exception à l'interdiction[265], de sorte que s'agissant des réseaux sociaux, seul un consentement explicite de l'utilisateur peut entrer en ligne de compte. Les considérations soulevées ci-avant concernant le traitement de données au sens de l'art. 22 par. 1, RGPD s'appliquent *mutatis mutandis* aux traitements de catégories particulières de données. Les responsables de traitement devraient mettre en place des mécanismes sollicitant une action positive des utilisateurs, tout en prenant garde à ce que le consentement soit éclairé. Autrement dit, les utilisateurs devraient être informés que, de leurs actions et comportements en ligne, des informations sensibles leurs sont inférées et qu'un ciblage publicitaire basé sur ces informations est possible.

2. Nécessaire à l'exécution du contrat d'utilisation

Si les exigences relatives au consentement ne sont pas remplies, le responsable du traitement peut se prévaloir d'autres bases juridiques pour légitimer le traitement de données à caractère personnel, notamment la nécessité à l'exécution du contrat selon l'art. 6 par. 1 point b) RGPD[266].

---

[258] SARGSYAN, p. 94.
[259] *Ibid*. *Cf.* aussi: BAERISWYL, in HK DSG, art. 4 N 74.
[260] GR29, WP259 rév.01, pp. 21-22.
[261] SARGSYAN, p. 94.
[262] Art. 9 RGPD.
[263] *Supra* Partie 1, Ch. 2, B, ch. 5.1.
[264] Art. 9 par. 1, RGPD.
[265] GR29, WP251 rév.01, p. 22.
[266] En droit suisse, l'exécution du contrat (art. 13 al. 2 let. a LPD) est un motif justificatif qui figure parmi les intérêts privés prépondérants pouvant entrer en ligne de compte pour justifier une atteinte illicite à la personnalité.

La nécessité à l'exécution du contrat constitue une base juridique au traitement de données de manière générale, mais également lorsque le traitement de données entre dans le champ d'application de l'art. 22 RGPD[267]. Deux conditions cumulatives sont à réaliser. La personne concernée doit participer au contrat et la condition de nécessité doit être remplie[268]. Si la participation de l'utilisateur au contrat d'utilisation du réseau social ne fait aucun doute, il n'en va pas aussi aisément du critère de nécessité. Le terme « nécessaire » ne signifie pas « indispensable »[269]. La nécessité renvoie à l'existence d'un lien direct et objectif entre le traitement de données et les objectifs contractuels escomptés de la personne concernée. En outre, le lien entre les données traitées et les opérations effectuées, d'une part, et l'exécution ou la non-exécution des services, d'autre part, est déterminant[270].

Le responsable du traitement doit pouvoir justifier la nécessité du traitement par rapport aux finalités contractuelles fondamentales et mutuellement comprises avec les utilisateurs[271]. Précisons encore que le seul fait de mentionner spécifiquement un traitement dans le contrat ne le rend pas nécessaire pour autant[272]. Il peut être nécessaire d'opérer une distinction entre le traitement effectué parce qu'il est prévu dans le contrat et celui effectué parce qu'il est nécessaire sans pour autant être expressément mentionné dans le contrat. Il convient de se poser la question de la nécessité du traitement de données à des fins de ciblage publicitaire pour assurer la bonne exécution du contrat d'utilisation. Sur ce point, nous partageons l'avis de SARGSYAN selon lequel les données des utilisateurs sont nécessaires à la fourniture des services, puisque les exploitants de réseaux sociaux ont besoin de ces données pour obtenir des revenus[273]. Ce motif ne devrait entrer en ligne de compte que dans un cadre limité[274] et nécessaire à la fourniture des services de base compris dans le contrat d'utilisation, comme la messagerie, la possibilité de contacts entre les utilisateurs et la diffusion de contenus générés par ceux-ci. Si la limite devait être ainsi fixée, les publicités ciblées n'entreraient *a priori* pas dans ce qui est nécessaire pour la fourniture des prestations de base.

Les réseaux sociaux proposent leurs services à titre gratuit aux utilisateurs selon un modèle économique type précis[275]. La gratuité des services est non seulement ce qui fait le succès de ces plates-formes mais est également la raison principale pour laquelle tant d'individus les utilisent. La mise à disposition gratuite des services figure parmi les prestations contractuelles de l'exploitant[276], puisqu'il s'agit d'un objectif contractuel escompté par les utilisateurs. Or, la publicité étant la source principale de revenus des exploitants, nous pouvons nous demander si celle-ci n'est pas nécessaire pour assurer la gratuité des services et, de surcroît, pour garantir l'exécution du contrat d'utilisation. Les frais de fonctionnement ne sont pas à négliger. En effet, les frais de gestion, d'élimination des contenus indésirables[277], sans compter les infrastructures, les data centers, les locaux et les charges salariales sont d'autant d'exemples éloquents.

---

[267] Art. 22 par. 2 point a) RGPD.
[268] DE TERWANGNE, in: *Le Règlement général sur la protection des données*, pp. 132-133.
[269] Arrêt CourEDH 5947/72 ; 6205/73 ; 7052/75 ; 7061/75 ; 7107/75 ; 7113/75 ; 7136/75 du 25 mars 1983 *Silver contre Royaume-Uni* par. 97. Dans le même sens: SCHULTZ, in: Kommentar DS-GVO, art. 6 N 36, qui stipule que le terme « Erforderlichkeit », tel qu'utilisé dans la disposition, ne doit pas être compris comme « einer absolut zwingenden Notwendigkeit » dont l'exécution du contrat ne serait pas possible sans ledit traitement.
[270] CEPD, p. 8.
[271] *Ibid.*
[272] WP219, pp. 16-17.
[273] SARGSYAN, p. 97 (nbp 732 a.i).
[274] *Idem,* pp. 96-97.
[275] *Supra* Partie 1, Ch. 1, B, ch. 2.
[276] Savoir si cette prestation est principale ou auxiliaire importe peu, étant donné que les deux cas de figure sont compris dans la disposition ; SCHULTZ, in: Kommentar DS-GVO, art. 6 N 27.
[277] MORITZ, p. 50.

S'il est manifeste que les activités d'observation, de suivi et de profilage des utilisateurs sortent du cadre de ce qui est nécessaire pour assurer le fonctionnement des services d'accès et d'utilisation de la plate-forme, il peut en aller différemment des revenus générés grâce à ces activités. Il y a lieu de déterminer la raison d'être exacte du contrat, soit son objectif fondamental, sa substance, car c'est à cette fin que l'analyse de la nécessité doit être effectuée[278]. Nous sommes d'avis que les revenus acquis grâce aux services publicitaires sont nécessaires pour couvrir les frais occasionnés et, partant, maintenir l'accès et l'utilisation gratuite des services. De plus, admettre que d'autres moyens pourraient être exigés des exploitants pour générer des revenus reviendrait à remettre en cause un modèle économique précisément choisi et largement répandu aujourd'hui. Bien que cette dernière argumentation ne saurait justifier à elle seule une nécessité à l'exécution du contrat[279], il convient cependant, à notre sens, de la prendre en considération.

Par ailleurs, les sommes astronomiques générées par la publicité[280] vont au-delà de ce dont le contrat de prestation de services a objectivement besoin, en terme monétaire, pour être opérant. Tous profits réalisés et dépassant le financement strictement nécessaire pour assurer la gratuité des services et l'exécution du contrat ne sauraient tomber sous le coup de ce fondement juridique. Pour y remédier, nous pourrions imaginer que le ciblage publicitaire soit nécessaire pour l'exécution du contrat (puisqu'il contribue à assurer la gratuité des services) mais qu'en revanche le profilage ne soit quant à lui pas nécessaire, ou en tout cas pas dans une aussi large mesure que celui effectivement effectué. Si l'on peut actuellement reconnaître qu'au vu du processus intrusif du profilage la nécessité du traitement ne peut être admise, la situation serait différente si les responsables du traitement mettaient en place des moyens moins excessifs. Ainsi, pour admettre la nécessité à l'exécution du contrat en tant que fondement juridique, nous pourrions exiger des exploitants de limiter leur niveau de profilage et ne traiter qu'un nombre limité de données (par exemple ne collecter que les données à l'interne de la plate-forme, ne plus recourir au profilage abstrait ou, plus restrictivement, ne traiter que les informations fournies par les utilisateurs). Nous pouvons également nous interroger sur la nécessité d'établir un profil-utilisateur, et donc d'effectuer un profilage, ou si une publicité contextuelle[282] ou limitée à l'activité du moment présent ne serait pas suffisante, sans qu'il soit nécessaire d'établir un profil et de conserver des données. Cette dernière considération pourrait constituer un juste milieu entre un profilage excessif et une simple publicité régulière[283]. En revanche, en ce qui concerne les catégories particulières de données au sens de l'art. 9 RGPD, celles-ci ne pourraient en aucun cas faire l'objet d'un traitement fondé sur la nécessité à l'exécution du contrat[284].

---

[278] GR29, WP217, p. 17. Les réseaux sociaux ont pour objectif de « créer une communauté et de rapprocher le monde ». Nous pouvons raisonnablement croire que cet objectif ne pourrait être atteint dans la même mesure si les services étaient payants.

[279] CEPD, p. 10.

[280] En 2018, Facebook aurait généré 16,6 billion de dollars US ; *Facebook ad revenue tops $16.6 billion, driven by Instagram, Stories,* disponible sur: https://martechtoday.com/despite-ongoing-criticism-facebook-generates-16-6-billion-in-ad-revenue-during-q4-up-30-yoy-230261 (consulté le 12.04.2019).

[282] *cf. supra* Partie 1, Ch. 1, B, ch. 3

[283] Citons à titre d'exemple le moteur de recherches Qwant, dont les publicités sont choisies en fonction du contenu recherché par l'internaute sans qu'aucune donnée personnelle ne soit collectée ; *cf.* Qwant, *Comment fonctionnent les publicités Qwants Ads ?,* disponible sur https://help.qwant.com/fr/aide/qwant-com/rechercher/comment-fonctionnent-les-publicites-qwant-ads/ (consulté le 02.07.2019). La publicité régulière, dont tout profilage est exclu, serait naturellement admise à titre de nécessité pour l'exécution du contrat. Les données des utilisateurs ne seraient pas traitées à des fins publicitaires, de sorte qu'un consentement ne serait pas requis.

[284] Cette possibilité est d'ailleurs implicitement exclue par la disposition.

Au vu de ce qui précède, les exploitants proposeraient aux annonceurs un ciblage certes moins affiné mais dont les publicités continueraient de générer des revenus. Les gains seraient évidemment moins conséquents mais les exploitants tireraient l'avantage de recourir à une alternative au consentement. Toutefois, même si ce fondement entrait en considération, cela ne dispenserait pas l'exploitant de respecter les principes généraux, en particulier le principe de transparence et le devoir d'information.

Les considérations avancées ci-dessus, bien que pertinentes, ne peuvent être admises de façon catégorique. Un contre-argument majeur peut en effet être soulevé, à savoir qu'un réseau social pourrait efficacement fonctionner sans ciblage publicitaire, puisque la publicité régulière permet de générer des revenus. Une évaluation des frais effectifs et des rentrées produites par la publicité régulière est déterminante. S'il s'avérait que les frais effectifs excédaient le produit des publicités régulières, on ne pourrait qu'admettre le ciblage publicitaire et les observations énoncées plus haut.

3. Intérêt légitime du responsable du traitement ou d'un tiers

Soulignons en premier lieu que l'intérêt légitime ou privé prépondérant ne peut entrer en considération lorsqu'on est en présence d'un traitement au sens de l'art. 22 par. 1, RGPD. Par conséquent, le présent chapitre sera pertinent lors de traitements de données à des fins de ciblage publicitaire dont le caractère intrusif n'est pas reconnu. À toutes fins utiles, précisons également qu'en cas de traitement de catégories particulières au sens de l'art. 9 RGPD, ce fondement juridique ne peut être invoqué. Le traitement de données à caractère personnel est permis lorsqu'il est nécessaire à la réalisation d'un intérêt légitime poursuivi par le responsable du traitement ou un tiers[285]. La notion d'intérêt légitime est large et couvre toutes sortes d'intérêts[286], tels que juridiques, économiques ou idéaux[287]. Notons que le responsable du traitement peut aussi bien invoquer un intérêt privé qu'un intérêt public de la collectivité[288].

3.1 Intérêt économique de l'exploitant du réseau social

La notion « d'intérêt » fait référence à l'enjeu poursuivi par le responsable du traitement, le bénéfice qu'il tire du traitement ou ce dont la société pourrait en tirer[289]. Cette notion est donc plus large que celle de « finalité ». S'agissant de notre problématique, la finalité du traitement correspond à la publicité ciblée en tant que telle tandis que l'intérêt de l'exploitant fait référence aux revenus générés par la publicité. Nous sommes en effet d'avis que l'intérêt poursuivi par l'exploitant d'un réseau social ne se limite pas à en savoir le plus possible sur ses utilisateurs dans le but de mieux cibler la publicité de ses clients (annonceurs). Si ce cas particulier figure certes parmi les finalités des politiques d'utilisation, il n'en demeure pas moins que, comme mentionné ci-avant, les finalités ne se regroupent pas nécessairement avec les intérêts poursuivis.

[285] L'art. 13 al. 2 LPD prévoit une liste non exhaustive d'intérêts privés prépondérants du responsable du traitement de données personnelles, par exemple lorsque le traitement est en relation directe avec la conclusion ou l'exécution d'un contrat, à condition que les données traitées concernent le cocontractant.
[286] GR29, WP217, p. 38.
[287] BUCHNER/PETRI, in: DS-GVO Kommentar, art. 6 N 146.
[288] GR29, WP217, p. 39.
[289] *Idem,* p. 26.

Pour lors, la question est de savoir quel est l'enjeu poursuivi par l'exploitant d'un réseau social à générer de la publicité ciblée. S'il est majoritairement admis qu'un intérêt purement économique ou commercial à générer du profit ou à éviter des dépenses supplémentaires ne peut entrer en ligne de compte pour justifier un traitement de données[290], il s'ensuit de l'analyse du fondement de la nécessité à l'exécution du contrat qu'un intérêt à générer des revenus existe[291]. Nous considérons ainsi qu'il y a un intérêt « public » ou « collectif » à ce que ces services soient gratuitement offerts au public et qu'un intérêt à générer des revenus dépasse ce qui est généralement traduit comme étant un intérêt purement économique de l'exploitant. Autrement dit, générer des revenus est nécessaire à garantir la gratuité de l'accès et de l'utilisation de la plate-forme, et cette garantie est d'intérêt public. La communauté sociale tire un profit économique non négligeable au fait qu'aucune contre-prestation pécuniaire ne soit requise. Bien que ce raisonnement aille à l'encontre de ce que la doctrine majoritaire et la jurisprudence[292] considèrent, il mérite réflexion. La possibilité d'invoquer cet intérêt en tant que fondement dépendra toutefois du résultat de la mise en balance des intérêts en présence.

3.2 Intérêts légitimes de par la loi

Le RGPD donne des exemples d'hypothèses où un traitement peut légitimement être effectué de par la loi. Il s'agira par exemple des traitements à des fins de prévention de la fraude, de prospection commerciale ou de marketing direct[293] ou visant à garantir la sécurité du réseau et des informations[294]. Le GR29 a souligné dans un de ses avis que le traitement à des fins de prévention de fraude peut comprendre l'établissement de profils[295]. Toutefois, le CEPD est d'avis contraire en considérant qu'un tel traitement est susceptible d'aller au-delà de ce qui est objectivement nécessaire à l'exécution du contrat[296].

S'agissant des réseaux sociaux, certains traitent des données dans le but de fournir des services sécurisés et fonctionnels, par exemple pour aider les personnes malvoyantes, détecter des activités dangereuses ou abusives, détecter des faux comptes ou des comptes piratés[297]. Il est cependant manifeste que les mesures mises en place pour collecter et traiter les données des utilisateurs à des fins de ciblage publicitaire vont bien au-delà du nécessaire pour assurer une sécurité du compte. Cependant, les revenus produits par la publicité pourraient justifier l'acquisition de machines ou logiciels, dont on devine un prix conséquent, toujours plus performants d'un point de vue sécuritaire. Dans ce cas-là, il convient d'intégrer cet aspect parmi les frais nécessaires à couvrir pour garantir l'exécution du contrat (*infra* Partie 2, Ch. 2, B, ch. 2).

---

[290] SARGSYAN, p. 97 (nbp 732) ; ANTREASYAN, pp. 139-140 ; BAERISWYL, *« Street View »,* p. 100: MEIER, p. 535.
[291] *Supra* Partie 2, Ch.2, B, ch. 2.
[292] SARGSYAN, p. 97 (nbp 732 i. f.) ; ANTREASYAN, pp. 139-140 ; BAERISWYL, *« Street View »,* p. 100: MEIER, p. 535. Le CEPD a également stipulé que « Bien qu'un tel traitement ne puisse soutenir la prestation d'un service, il est distinct de la finalité objective du contrat entre l'utilisateur et le prestataire de services et n'est donc pas nécessaire à l'exécution du contrat ». Ne partageant pas cet avis, nous considérons que l'accès gratuit aux services est une finalité objective du contrat, à côté du libre accès à la plate-forme et son utilisation ; CEPD, p. 13. Dans un arrêt Google Street View du TF (ATF 138 II 346 du 31 mai 2012, consid. 10.4), le TAF avait considéré que la gratuité des services ne pouvait être retenu comme un intérêt public ou privé prépondérant, de sorte que cela n'était qu'un prétexte quant au réel intérêt de nature économique ou financier des services offerts par Google Street View.
[293] Consid. n° 47 RGPD.
[294] Consid. n° 49 RGPD.
[295] GR29, WP217, p. 17.
[296] CEPD, p. 12.
[297] Conditions d'utilisation Facebook, disponible sur: https://www.facebook.com/legal/terms/update (consulté le 06.04.2019) ; Politique de confidentialité Twitter, disponible sur: https://twitter.com/fr/privacy (consulté le 06.04.2019).

Pour ce qui de la prospection directe[298], une protection particulière est apportée en référence à la protection à l'image professionnelle, à la liberté entrepreneuriale, à la liberté d'expression et d'information[299]. Les responsables du traitement ayant pour but de promouvoir la vente de biens ou la prestation de services[300] peuvent invoquer cet intérêt légitime. De telles considérations pourraient potentiellement entrer en ligne de compte s'agissant de l'intérêt des annonceurs à recourir aux services publicitaires des réseaux sociaux, puisque les intérêts des exploitants à la publicité ciblée ne sont pas de nature à promouvoir un produit ou un service mais de générer des revenus afin que les utilisateurs puissent gratuitement utiliser la plate-forme[301].

3.3 Expérience personnalisée de l'utilisateur

Le RGPD ne précise pas si un responsable du traitement peut invoquer l'intérêt de la personne concernée elle-même. La doctrine suisse admet qu'un tel intérêt peut entrer en ligne de compte et être invoqué[302]. Nous nous alignons sur cette position. Les réseaux sociaux défendent souvent leurs pratiques par le bien-être des utilisateurs, l'expérience personnalisée ou l'amélioration des services[303]. Les membres de la communauté peuvent avoir un intérêt à recevoir de la publicité pertinente plutôt que « régulière » [304]. Une difficulté serait de savoir si la personnalisation des services s'étend à la publicité ciblée ou non. Le CEPD ne mentionne pas, dans ses lignes directrices, la publicité ciblée dans la section relative à la personnalisation des services, celle-ci faisant l'objet d'un chapitre séparé[305]. Partageant ce raisonnement, nous considérons dès lors que la publicité ciblée ne peut être invoquée en tant qu'intérêt légitime à offrir une expérience-utilisateur personnalisée[306].

3.4 Balance des intérêts

Les intérêts légitimes poursuivis par le responsable du traitement, quoi que tenus pour admis, ne peuvent prévaloir les intérêts, les droits et les libertés fondamentales des utilisateurs[307]. Une mise en balance des intérêts en présence est donc nécessaire afin de déterminer si l'art. 6 par. 1 point f) RGPD peut servir de fondement juridique au traitement de données. Pour ce faire, il convient de tenir compte de la forme, du contenu et de la valeur des données concernées[308].

---

[298] Consid. n° 47 RGPD ; SCHULTZ, in: Kommentar DS-GVO, art. 6 N 54.
[299] SCHULTZ, in: Kommentar DS-GVO, art. 6 N 64.
[300] BUCHNER/PETRI, in: DS-GVO Kommentar, art. 6 N 175.
[301] Dans le même sens: Tribunal administratif de Bayreuth décision du 8 mai 2018 - B 1 S 18. 105, N 9.
[302] MEIER, p. 536.
[303] MAYER/MITCHELL, p. 417 ; LEONARD, p. 8.
[304] OBERLIN, *Teil I*, p. 18.
[305] CEPD, pp. 12-14.
[306] Dans le cas contraire, les procédés de collecte et d'analyse mis en place afin de cibler au mieux les publicités dépassent les informations dont l'exploitant auraient besoin pour diffuser une publicité présentant un minimum de pertinence pour les utilisateurs. À cela s'ajoute que la personnalisation des publicités ne saurait primer une violation de la vie privée des utilisateurs et un traitement potentiellement intrusif de leurs données. Dans le même sens: ESTEVE, p. 43.
[307] Art. 6 par. 1 point f) RGPD.
[308] BUCHNER/PETRI, in: DS-GVO Kommentar, art. 6 N 149.

3.4.1 Mise en balance avec les intérêts économiques de l'exploitant

Selon les considérations du GR29, le fait qu'un responsable de traitement agisse dans son propre intérêt légitime, mais aussi dans l'intérêt de la collectivité, peut donner un poids plus important à cet intérêt[309]. En matière de publicités ciblées, les exploitants des réseaux sociaux ont certes un intérêt légitime à offrir des services publicitaires à des annonceurs afin de générer du revenu, cela ne signifie pas pour autant qu'ils peuvent invoquer cet intérêt pour justifier le recours à des technologies de collecte massive dans le but d'enrichir considérablement les bases de données pour créer des profils complexes et prédire des préférences. Un tel processus de profilage constitue à notre sens une violation de la vie privée des utilisateurs et leur intérêt à ne pas faire l'objet de traitements intrusifs prévaut sur l'intérêt poursuivi par le responsable du traitement[310]. Précisons toutefois que s'agissant de l'audience personnalisée[311], une violation dans la vie privée est moins conséquente, voire infime, puisqu'une relation entre l'utilisateur et l'annonceur est *a priori* établie.

Néanmoins, on ne saurait être radical en affirmant une « non légitimité » catégorique à ce motif. Un traitement de données à des fins de ciblage publicitaire pourrait être justifié par les intérêts économiques du réseau social si et seulement si un équilibre est opéré. Par exemple, le ciblage pourrait n'être fondé que sur les données livrées directement par l'utilisateur, voire sur les données collectées uniquement à l'interne de la plate-forme. Pour établir un équilibre, l'exploitant devrait mettre en place des garanties et mesures adéquates, par exemple en offrant aux utilisateurs davantage de possibilités de limiter facilement le traitement des données à certaines catégories et de s'opposer à tout traitement à des fins de publicités ciblées[312]. Il devrait également limiter, de lui-même, l'ampleur des activités de profilage. Le principe de transparence et le devoir d'information ont également un rôle important. Un intérêt pourra d'autant plus être qualifié de légitime si le traitement en question jouit d'une transparence accrue vis-à-vis des personnes concernées[313].

Soulignons aussi l'importance de l'intérêt collectif à la gratuité des services. Si un équilibre avec les intérêts, les droits et les libertés fondamentales des utilisateurs est opéré, l'intérêt collectif renforcera la légitimité des traitements à des fins publicitaires fondée sur un intérêt économique à générer des revenus.

---

[309] Contrairement au RGPD, l'art. 13 al. 2 LPD mentionne expressément qu'une atteinte à la personnalité peut être justifiée « par un intérêt privé ou public prépondérant ». L'intérêt est public s'il procure un avantage à la collectivité ou à une multitude de personnes. Dans les relations privées, l'intérêt public est en général invoqué pour soutenir un intérêt privé prépondérant ; MEIER, pp. 533-534 ; HK-ROSENTHAL, art. 13 N 20 ; RAMPINI, in: BSK DSG/BGO, art. 13 N 47. Mentionnons à titre d'exemple le cas de la surveillance d'un assuré admise pour justifier un intérêt collectif des assurés à ne pas payer des primes trop élevées ; ATF 136 III 410 - 5A_57/2010 du 2 juillet 2010, consid. 2.2.3 et 4.1 ; Arrêt du TF 8C_239/2008 du 17 décembre 2009.

[310] Pour citer les propos tenus par le GR29, « il serait difficile pour les responsables du traitement de justifier le recours à des intérêts légitimes (…) pour des pratiques intrusives du profilage et de suivi à des fins de marketing ou de publicité, par exemple, celles qui impliquent le suivi d'individus sur plusieurs sites web, emplacements, dispositifs (..). » ; GR29, WP251 rév.01, p. 16.

[311] *Supra* Partie 1, Ch. 2, B, ch 5.1.

[312] Un droit d'opposition est reconnu en vertu de l'art. 21 par. 1, RGPD lorsque le traitement est fondé sur un intérêt légitime du responsable de traitement ou d'un tiers en vertu de l'art. 6 par. 1 point f) RGPD. L'art. 21 par. 2, RGPD est également pertinent s'agissant d'un droit d'opposition reconnu en tout temps en cas de traitements de données à des fins de prospection, y compris le profilage effectué à telles fins. Voir: OBERLIN, *Teil 1*, p. 19.

[313] Voir: GR29, WP217, p. 48.

C. Qualification et responsabilité: aperçu d'une problématique pertinente

Au vu du caractère potentiellement illicite du traitement de données à des fins de ciblage publicitaire, il est intéressant de s'interroger sur la qualification des principaux intéressés, respectivement sur leur responsabilité. S'il est évident que l'exploitant d'un réseau social est responsable du traitement de données s'agissant de l'accès et la mise à disposition de la plate-forme aux utilisateurs, la question de sa qualification peut se poser en ce qui concerne les traitements des données à des fins de ciblage publicitaire. Qualifier l'exploitant de responsable du traitement ou de sous-traitant n'est pas sans conséquence en termes de responsabilité. La qualification des réseaux sociaux en tant que sous-traitant pour le compte des entreprises recourant à leurs services publicitaires a été soulevée dans une décision du 8 mai 2018 par le Tribunal administratif de Bayreuth[314]. Cette affaire concernait le cas précis du recours aux services d'audiences personnalisées[315]. Le Tribunal a évalué le traitement de données, le rôle respectif de l'exploitant et de l'annonceur dans le processus ainsi que l'étendue de leurs pouvoirs de décision. Il a en outre été considéré que l'exploitant n'agissait pas seulement en tant que sous-traitant en suivant des instructions précises de l'annonceur mais prenait des décisions propres quant aux profils-utilisateurs à analyser pour la campagne publicitaire. L'exploitant agit, par conséquent, également en tant que responsable de traitement[316] et possède une marge d'appréciation et de discrétion non négligeable qui va-delà d'une fonction purement auxiliaire de traitement de données[317]. L'annonceur et l'exploitant sont dès lors responsables conjoints de traitement au sens de l'art. 26 RGPD[318].

Dans une autre affaire de la CJUE du 5 juin 2018[319], une coresponsabilité a également été prononcée mais cette fois-ci entre l'exploitant du réseau social et l'administrateur d'une page fan. La CJUE, retenant une définition large du responsable du traitement[320], a ainsi jugé que bien que l'administrateur d'une page fan ne collecte pas lui-même les données, il offre néanmoins la possibilité à Facebook de recourir à des techniques de suivi en ligne des utilisateurs dans le but de collecter des données[321]. Cette collecte servira, d'une part, à établir des statistiques mises à disposition de l'administrateur et, d'autre part, à enrichir les bases de données utilisées pour le ciblage publicitaire. L'administrateur contribue par conséquent au traitement des données des visiteurs de sa page[322]. Dans une autre affaire, la Cour a précisé qu'il n'était pas nécessaire pour des responsables conjoints du traitement d'avoir chacun accès aux données à caractère personnel[323]. La Cour a confirmé les conclusions prises par son avocat général dans lesquelles il précise qu'une responsabilité conjointe ne signifie pas qu'elle soit équivalente[324].

---

[314] Tribunal administratif de Bayreuth, décision du 08. 05. 2018 - B 1 S 18. 105.
[315] *Cf. supra* Partie 1, Ch. 2, B, ch. 5.1.
[316] Tribunal administratif de Bayreuth, décision du 08. 05. 2018 - B 1 S 18.105, N 9 ; *Cf.* aussi: OBERLIN, *Teil 2*, p. 70.
[317] Tribunal administratif de Bayreuth, décision du 08. 05. 2018 - B 1 S 18.105, N 49.
[318] OBERLIN, p. 70.
[319] CJUE, Arrêt C-210/16 du 5 juin 2018. *Cf*. aussi: BAERISWYL, *Datenschutzrecht*, p. 451.
[320] CELLINA, N 5.
[321] CJUE, Arrêt C-210/16, point 35. *Cf.* aussi: CELLINA, N 7-9.
[322] CJUE, Arrêt C-210/16, point 36 ; *Cf*. aussi les conclusions de l'avocat général dans l'affaire C-210/16, points 57, 69 et 72 et CELLINA, N 8-10.
[323] CJUE, Arrêt C-25/17 du 10 juillet 2018, points 68 à 72 (affaire Jehovan todistajat).
[324] Conclusions de l'avocat général dans l'affaire C-210/16, point 75 ; CJUE, Arrêt C-210/16, point 43.

Selon la Cour, l'administrateur d'une page fan prend part à la détermination des finalités et des moyens du traitement de données à caractère personnel et doit de ce fait être qualifié de responsable du traitement joint avec Facebook[325]. Dans une autre affaire pertinente en la matière et toujours pendante[326], l'avocat général est arrivé à la conclusion qu'une entreprise intégrant des plugins sociaux sur son site web est un responsable conjoint du traitement de données avec l'exploitant du réseau social[327]. Au vu de ces affaires, l'élément déterminant serait alors la « possibilité » octroyée à l'exploitant de collecter des données.

Appliquer ces raisonnements à notre problématique s'avère pertinent. Bien que l'exploitant du réseau social s'occupe de la collecte des données, du profilage et de la diffusion des publicités au bon endroit et au bon moment, le rôle de l'annonceur est également significatif. En effet, il est celui qui choisit un objectif commercial, qui identifie l'audience souhaitée sur la base d'une multitude de critères[328] et finalement qui crée la publicité. À ce titre, nous pourrions raisonnablement admettre que l'annonceur est celui qui, certes ne traite pas les données à proprement parler, ni ne fournit les moyens de traitement, mais participe aux processus de ciblage publicitaire. L'annonceur qui exploite activement des outils tels que les pixels ou les plugins sociaux fournit au réseau social l'opportunité d'observer et de suivre l'activité et le comportement des utilisateurs en ligne et favorise la collecte de données à caractère personnel. Tout comme l'administrateur d'une page fan, les annonceurs ont également à leur disposition des statistiques sur les performances de leurs publicités fournies par le réseau social. Ce qui leur permet d'opérer un choix d'audience en fonction de profils établis dans les statistiques. Dès lors, en ayant la possibilité de définir les paramètres de ciblage déterminants pour les profils qui feront l'objet du traitement de données, nous pouvons considérer l'annonceur comme un responsable du traitement joint. L'objectif d'une définition large de « responsable du traitement » est de garantir une protection complète et efficace aux personnes concernées[329].

Conformément à la législation sur la protection des données, les responsables de traitement doivent conjointement décider qui est responsable des obligations, et desquelles, qui sont prévues et qu'ils doivent satisfaire. Une autre importante conséquence de telles considérations, y compris à propos des affaires citées ci-avant, est que les droits des personnes concernées peuvent être exercés tant auprès de l'exploitant qu'auprès de l'administrateur de la page fan, respectivement de l'annonceur.

[325] CJUE, Arrêt C-210/16, points 31 et 39.
[326] CJUE, Arrêt C-40/17, demande déposée le 26 janvier 2017 (affaire pendante).
[327] Conclusions de l'avocat général dans l'affaire C-40/17, points 66-70.
[328] La jurisprudence allemande n'a toutefois pas considéré que la sélection de critères particuliers par l'annonceur constituait un traitement de données à caractère personnel. Voir: Tribunal administratif de Bayreuth, décision du 08. 05. 2018 - B 1 S 18.105. A l'instar de cette jurisprudence, nous considérons qu'une telle sélection de critère est décisive pour le traitement de données à caractère personnel à des fins publicitaires et de surcroît y participe. *Cf*. aussi: Conclusions de l'avocat général dans l'affaire C-210/16, point 57.
[329] CJUE, Arrêt C-210/16, point 28.

CONCLUSION

Les risques que le traitement de quantités massives de données sont susceptibles d'engendrer sont méconnus. Le recours au *data mining* ou autres technologies d'optimisation du profilage est intrusif. Comme le stipule LEONARD, « c'est un peu comme s'il se promenait avec, constamment, une caméra dirigée sur lui et un micro permettant de le rendre transparent pour l'observateur »[330]. Le modèle économique basé sur le traitement de données à des fins publicitaires, bien que reconnu, ne saurait comporter aucune limite. L'exigence imposée par le RGPD d'une base juridique légitimant le traitement de données est une limite que les responsables de traitement doivent respecter. Retenons que les exigences en matière de protection des données n'ont pas été instituées pour freiner les nouvelles technologies mais plutôt dans le but de réguler et encadrer leur usage et protéger la personnalité des personnes concernées. L'ordre des fondements juridiques présenté à l'art. 6 RGPD n'est d'aucune pertinence, de sorte qu'aucune hiérarchie n'existe entre eux. En l'état actuel des activités de profilage et de l'ampleur de la collecte des données, le consentement semble être la base juridique la plus appropriée, bien que critiquée pour être un échappatoire au respect des règles de protection des données[331]. La réalisation des exigences d'un consentement libre, éclairé, spécifique et univoque dépend essentiellement de l'information fournie aux personnes concernées. Il est vrai que les politiques d'utilisation des réseaux sociaux posent particulièrement problème en ce qui concerne la clarté et la spécificité du consentement. Les améliorations effectuées sont toutefois à prendre en compte. Nonobstant, les entreprises qui recourent au profilage doivent fournir davantage de précisions quant au fonctionnement du processus. Une explication simple par étapes du profilage, de la collecte à l'inférence de nouvelles informations aux profils-utilisateurs, est nécessaire. Sans toutefois noyer l'utilisateur lambda dans un jargon technique et informatique incompréhensible. Il devrait avoir le choix d'accepter ou non que ses données soient traitées à des fins publicitaires lors de leur inscription, et non *a posteriori* par le biais de ses paramètres.

La nécessité à l'exécution du contrat et l'intérêt légitime sont deux fondements juridiques sur lesquelles le traitement à des fins de publicités ciblées pourrait reposer. Dans le premier cas, la publicité sert à assurer l'exécution d'une obligation contractuelle. Dans le second, celle-ci apparaît comme un intérêt « public » ou « collectif » à ce que l'accès aux services demeure gratuit. Ces fondements sont des pistes qui méritent d'être étudiées, en particulier parce qu'ils ont l'avantage de servir d'alternatives au consentement et aux difficultés à répondre aux exigences s'y rapportant. Il est cependant nécessaire d'établir un équilibre. L'exploitant du réseau social devrait limiter le traitement de données, notamment le profilage, et porter une attention particulière au principe de transparence et au devoir d'information pour s'en prévaloir. Il devrait en outre renoncer au traitement de catégories particulières de données au sens de l'art. 9 RGPD à défaut de consentement et mettre à disposition des utilisateurs des moyens de contrôler le traitement de leurs données et de s'y opposer. La possibilité de s'y opposer réduit la gravité de l'atteinte au droit à l'autodétermination informationnelle. À cet égard, le consentement garde son importance pour tout traitement de données qui n'est pas nécessaire à l'exécution du contrat ou ne tombe sous le fondement de l'intérêt légitime.

Lorsque l'exploitant a pour objectif uniquement d'optimiser le ciblage publicitaire, sans égard à une quelconque nécessité pour le contrat, les alternatives au consentement ne peuvent servir de fondement juridique justifiant le traitement de données personnelles.

---

[330] LEONARD, p. 5.
[331] SARGSYAN, pp. 92 et 102.

Quant aux avantages et inconvénients du fondement de l'intérêt légitime du responsable du traitement ou d'un tiers, la notion d'intérêt légitime est plus large que la notion de finalité et ne se limite par conséquent pas à la publicité ciblée en tant que telle mais peut s'étendre aux revenus générés par cette dernière. Il n'y a en outre aucune exigence de nécessité à démontrer. La marge d'appréciation conférée par la disposition s'avère à la fois utile, puisqu'elle permet une interprétation large de la notion d'intérêt, mais également délicate, puisqu'elle contribue à l'insécurité juridique et rend le champ d'application de ce fondement pour l'heure encore flou. La pesée des intérêts à effectuer rend son application d'autant plus restreinte. Nonobstant, ce fondement est d'une importance particulière dans la pratique, surtout en présence de technologies de profilage, de tracking ou de data mining susceptibles de traiter d'énormes quantités de données et où il est difficile de recueillir un consentement[332]. L'intérêt collectif est un aspect supplémentaire à ne pas négliger dans l'appréciation de ce motif, puisqu'il contribue à servir les intérêts de milliards d'utilisateurs. Nous sommes d'avis qu'une plus grande importance devrait être portée à l'égard de ce fondement juridique pour justifier le traitement des données à des fins de ciblage publicitaire.

Si un nombre important d'utilisateurs venait à s'opposer aux traitements de données à des fins publicitaires, de sorte que la publicité régulière ne permette pas, à elle seule, d'assumer le financement des charges nécessaires, les exploitants pourraient proposer leurs services contre rémunération[333]. Toutefois, lors de son audition devant le Sénat américain, Mark Zuckerberg a répondu à des sénateurs qui lui avaient demandé s'il envisageait de rendre Facebook payant, afin de mieux garantir le respect de la vie privée de ses utilisateurs « *Pour être clair, nous ne proposons pas à l'heure actuelle d'option payante pour ceux qui ne souhaiteraient pas voir de publicités. Nous voulons un service gratuit [pour] que tout le monde puisse se l'offrir* »[334]. Il est vrai qu'un tel changement reviendrait à dénier l'essence et la légitimité du modèle économique de la gratuité des services.

En ce qui concerne toute collecte ou utilisation de données dépassant la stricte nécessité du bon fonctionnement de la plate-forme sociale, il serait souhaitable d'incorporer des mécanismes d'opt-in pour respecter les exigences relatives au consentement. Ce modèle présente un traitement minimal des données, où chaque accroissement des paramètres de confidentialités serait préalablement soumis à l'approbation explicite de l'utilisateur du réseau social. Le modèle d'opt-in est orienté vers une plus grande transparence et une plus grande prise de conscience de la personne concernée de ce à quoi elle consent. Un mécanisme d'opt-in est par ailleurs conforme au principe « *privacy by default* » prévu à l'art. 25 par. 2 RGPD qui veut que seules les données à caractère personnel nécessaires au regard de chaque finalité soient traitées. Le responsable du traitement ne peut dès lors pas traiter, par défaut, plus de données que ce qui est nécessaire et limité pour la finalité spécifique du traitement[335]. Les paramètres établis par défaut doivent être favorables à la protection des données. Comme l'indique l'art. 25 par. 2 RGPD, cela s'applique tant à la quantité des données traitées, qu'à l'étendu des traitements effectués, leur durée de conservation et leur accessibilité. C'est à la personne concernée de configurer les paramètres et de les accroître à sa convenance par une action positive, soit un mécanisme d'opt-in.

---

[332] MEIER, p. 159. L'auteur stipule précisément que « le nombre de données collectées et traitées quotidiennement ne permet plus d'exiger systématiquement un consentement, alors que le respect strict du droit à l'autodétermination (…) commanderait au contraire d'exiger (…) ce motif justificatif du traitement ».

[333] À l'exemple de YouTube Premium, où le visionnage de vidéos n'est plus accompagné de publicités.

[334] TUAL/SIGNORET, *Facebook: cinq moments forts de l'audition de Mark Zuckerberg,* disponible sur: https://www.lemonde.fr/pixels/article/2018/04/11/facebook-cinq-moments-forts-de-l-audition-de-mark-zuckerberg-devant-le-senat-americain_5283968_4408996.html (consulté le 11 février 2019).

[335] DE TERWANGNE, in: *Le Règlement général sur la protection des données*, p. 390.

Le principe *« privacy by default »* fait partie intégrante du principe « *privacy by design* » énoncé à l'art. 25 par. 1 RGPD[336] et selon lequel les principes relatifs à la protection des données doivent être mis en œuvre de façon effective par des mesures techniques et organisationnelles dès la conception du traitement[337]. Un mécanisme d'opt-out[338], qui donnerait la possibilité aux utilisateurs de refuser que ses données soient traitées à des fins de publicités ciblées, semble à tout le moins être une solution *minimale* guère suffisante. L'opt-out se réfère plutôt à l'absence de réaction des personnes concernées plutôt qu'à une action positive de leur part. De surcroît, la volonté des utilisateurs est supposée, ce qui ne saurait répondre aux exigences relatives à la validité du consentement.

La proposition de règlement ePrivacy[339] (ci-après : P-ePrivacy), abrogeant la directive 2002/58/CE du 12 juillet 2002, prévoit également les principes *« privacy by design »* et *« privacy by default »* (consid. n° 23 P-ePrivacy). Cela pourrait notamment avoir pour conséquence que les cookies et autres outils de suivi de tiers qui permettent le partage d'informations ne devraient désormais être autorisés qu'après une action positive de l'internaute puisqu'ils ne sont pas nécessaires, et non pas par défaut[340]. Il sera intéressant de voir comment cette exigence sera mise en œuvre, pour deux raisons en particulier. La première tient au fait qu'en s'inscrivant à une plate-forme sociale, l'utilisateur accepte, en général, que l'exploitant collecte ses données, y compris au travers des techniques de suivi en ligne intégrées sur des sites web tiers. La seconde raison tient à l'hypothèse où une majorité d'internautes, si ce n'est pas tous, ne modifient pas leurs paramètres par défaut de façon à ce que les cookies et autres techniques de suivi de tiers soient autorisés. Se pose alors la question de savoir dans quelle mesure les réseaux sociaux pourraient être (ou ne pas être) atteints par une telle configuration.

[336] *Idem*, p. 391.
[337] Le consid. n° 75 RGPD précise que le responsable du traitement, pour respecter ces principes, devraient adopter des mesures consistant, entre autres, à réduire à un minimum le traitement des données, à pseudonymiser les données et à garantir la transparence.
[338] Le modèle d' « opt-out » est en général préconisé par les responsables de traitement car il présente l'avantage qu'aucune action positive de la personne concernée est requise. En outre, le consentement est considéré comme avoir été donné dès le départ, à défaut d'intervention de la personne concernée en vue d'effectuer des modifications, que ce soit par ignorance ou imprudence. Il s'apparente au consentement implicite, or celui-ci n'est pas admis. *Cf.*: BUCHNER, p. 4 et *supra* Partie 2, Ch. 2, B, ch. 1.2.2.
[339] Proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58CE (règlement « vie privée et communications électroniques ») COM/2017/010 final - 2017/03 (COD).
[340] Conformément aux consid. n° 21 et 22 P-ePrivacy, une exception est faite « aux situations qui n'impliquent aucune intrusion, ou qu'une intrusion limitée, dans la vie privée ». Ce sera le cas lorsque la technique utilisée est strictement nécessaire en regard du service expressément demandé par l'utilisateur. Voir *supra* Partie 1, Ch. 2, B, ch. 3.1.1.

Annexe

- Formulaire Code de déontologie en matière d'emprunts, de citations et d'exploitation de sources diverses