Auteur : Mlle Morgane BERNARD, élève avocate au cabinet CONSTELIUS à Prague, République tchèque
Date : le 22 septembre 2020

PANORAMA DES DÉCISIONS RENDUES PAR LA CJUE EN MATIÈRE DE DONNÉES PERSONNELLES

Cet article a pour vocation de présenter un panorama des décisions rendues par la Cour de Justice de l'Union Européenne, du début des années 2000 jusqu'à tout récemment, en juillet 2020.
Cette jurisprudence s'inscrit dans la volonté européenne de garantir un véritable système de protection des données, uniformisé et efficace, sous l'empire de la directive 95/46/CE et plus récemment du Règlement Général pour la Protection des Données (RGPD).
La division a été faite en fonction de thèmes qu'il est possible de dégager à la lecture des arrêts : tout d'abord, des arrêts permettant de donner une définition de la notion de données à caractère personnel (1), puis sur la notion de traitement de données à caractère personnel (2), également sur l'hypothèse de transfert des données à caractère personnel vers des pays tiers (3) et enfin, sur les autorités nationales de contrôle et la portée de leur exigence d'indépendance (4).

1. Notion de « données à caractère personnel »

☛ Arrêt Breyer, 19 octobre 2016

Les services fédéraux allemands avaient pris la précaution d'enregistrer les coordonnées des adresses IP des internautes qui consultaient leurs sites afin de se prémunir contre des attaques dites « pirates ». Les adresses étaient collectées dans des fichiers journaux et pouvaient être extraites afin de faciliter d'éventuelles poursuites pénales.

Un ressortissant Allemand s'était opposé à l'administration allemande par un recours visant à ce qu'il fût fait interdiction à la République fédérale d'Allemagne de conserver ou de faire conserver par des tiers des données informatiques qui étaient transmises au terme de chaque consultation des sites Internet des services fédéraux allemands.

La question qui se posait était de savoir si une adresse IP pouvait être qualifiée de donnée personnelle permettant d'identifier un individu ?

La Cour avait constaté qu'une adresse IP dynamique, enregistrée par un fournisseur de services de médias en ligne à l'occasion de la consultation par une personne d'un site Internet que ce fournisseur rend accessible au public, constitue, à l'égard dudit fournisseur, une donnée à caractère personnel (article 2 directive 95/46/CE), lorsqu'il dispose de moyens légaux lui permettant de faire identifier la personne concernée grâce à des informations supplémentaires dont dispose le fournisseur d'accès à Internet de cet individu.

☛ **Arrêt Nowak, 10 décembre 2017**

Monsieur Nowak avait passé un examen organisé par l'ordre irlandais des experts-comptables, auquel il avait échoué. Il avait formulé la demande qu'on lui communique l'ensemble des données à caractère personnel le concernant, auprès de l'Ordre des experts comptables qui les détenait. Certains documents avaient été communiqués, à l'exception de la copie d'examen de l'étudiant. Le motif à ce refus était qu'elle ne contenait pas de données à caractère personnel le concernant, au sens de la loi sur la protection des données.

La Cour de Justice a été saisie sur le point de savoir si les réponses écrites fournies par un candidat lors d'un examen professionnel et les éventuelles annotations de l'examinateur s'y rapportant constituent des données à caractère personnel concernant le candidat, au sens de la directive européenne 95/46/CE ?

La Cour a considéré que le contenu des réponses reflète notamment son niveau de connaissance et de compétences, mais aussi son processus de réflexion ou son esprit critique et qu'elles constituaient ainsi des informations liées à sa personne.
Elle va même plus loin dans le raisonnement en assimilant les annotations de l'examinateur sur la copie du candidat à des informations relatives à ce dernier puisqu'elles reflètent l'appréciation d'un examinateur sur ses performances individuelles. Ces annotations ont, par ailleurs, précisément pour finalité de documenter l'évaluation par l'examinateur des performances du candidat.

Au vu de tous ces éléments, la Cour a conclu que les réponses écrites fournies par un candidat lors d'un examen professionnel et les éventuelles annotations de l'examinateur relatives à ces réponses constituent des données à caractère personnel, au sens de l'article 2, sous a), de la directive 95/46/CE.

2. Notion de « traitement » de données à caractère personnel

☛ **Arrêt Lindqvist, Cour réunie en Assemblée Plénière, 6 novembre 2003**

Dans une Église protestante de Suède, une travailleuse bénévole avait créé des pages internet qui mentionnaient des personnes travaillant avec elles, et donc certaines de leurs données personnelles apparaissaient sur le site. La bénévole avait été condamnée à payer une amende pour le non-respect de la déclaration écrite préalable obligatoire auprès de l'organisme suédois responsable de la protection des données transmises par voie informatique et pour leur utilisation et leur transfert vers des pays tiers.

La question qui se posait à la Cour de justice était de savoir si Mme Lindqvist s'était livrée à un « traitement de données à caractère personnel, automatisé en tout ou en partie », au sens de la directive 95/46/CE.

La Cour a effectivement constaté que le site internet faisait référence à des personnes grâce à leur nom, leur numéro de téléphone, leurs conditions de travail ou même leurs passe-temps et qu'il s'agissait donc de « *traitement de données à caractère personnel, automatisé en tout ou en partie* ». Bien que les données soient utilisées pour des activités bénévoles ou religieuses, il ne s'agissait pas d'une des exceptions au champ d'application de la directive (i.e. sécurité publique ou activités exclusivement personnelles ou domestiques).

☛ Arrêt Google & Google Spain, Cour réunie en Grande chambre, 13 mai 2014

Un ressortissant espagnol avait introduit une réclamation auprès de l'agence espagnole de protection des données (AEPD) et de Google et Google Spain car il avait constaté que lorsque son nom était tapé sur ce moteur de recherche, les résultats affichaient des liens vers le journal La Vanguardia, concernant des informations sur une vente aux enchères organisée pour recouvrer ses dettes.
Il demandait ainsi au journal soit que les pages soient modifiées ou supprimées soit que ses données soient protégées. Il demandait également à Google que ses données personnelles n'apparaissent plus lorsque son nom était recherché.
L'AEPD avait accueilli la demande portée contre Google et Google Spain et leur avait demandé de prendre des mesures afin que les données soient retirées de leur index et que leur accès soit rendu impossible à l'avenir. Les sociétés ont introduit des recours et les juridictions espagnoles ont interrogé directement la Cour de justice.

Dans cet arrêt, la Cour de justice a pu préciser la notion de « traitement de données à caractère personnel » selon les dispositions de la directive 95/46/CE.

La Cour a indiqué qu'un moteur de recherche qui permettait de trouver des informations émises par des tiers, qui les triait, les stockait et les mettait à disposition des internautes selon un ordre de pertinence devait être qualifié de traitement de données à caractère personne dès alors que toutes ces informations contiennent des données à caractère personnel.

3. Transfert des données à caractère personnel vers des pays tiers (hors de l'Union Européenne et du champ d'application du règlement RGPD)

☛ Arrêt Schrems, Cour réunie en Grande chambre, 6 octobre 2015

Un étudiant autrichien en droit s'était plaint, auprès de l'autorité Irlande de protection des données, que ces dernières, récoltées par Facebook Irlande étaient envoyées à des serveurs américains de la firme. Selon lui, les lois américaines ne permettaient pas d'obtenir une protection suffisante des données (en écho aux affaires révélées par Edward SNOWDEN, quelques mois plus tôt).

Sa plainte est portée devant la Commission Européenne, qui la rejette au motif que le régime dit de la « sphère de sécurité » (« *Safe Harbor* ») mis en place par l'Europe offre un niveau suffisant de protection pour les données transférées des usagers.

La Cour de Justice de l'Union Européenne est finalement interrogée, par la Haute Cour d'Irlande, sur la capacité de la Commission à constater qu'un pays tiers assure un niveau de protection de données adéquat.

La Cour invalide finalement la décision de la Commission, et ce dans son intégralité.
Elle explique tout d'abord que la Commission devait se charger constater, de manière effective, que le pays tiers assurait un niveau de protection équivalent à celui qui était garanti dans le droit de l'Union Européenne.

De plus, la Cour indique que la décision de la Commission ne saurait « *ni annihiler ni réduire les pouvoirs expressément reconnus aux autorités nationales de contrôle par l'article 8 paragraphe 3 de la Charte* » et que « *les autorités nationales de contrôle, saisies par une personne d'une demande relative à la protection de ses droits et libertés à l'égard du traitement des données à caractère personnel la concernant, doivent pouvoir examiner, en toute indépendance, si le transfert de ces données respecte les exigences posées par [la] directive* ».

Enfin, sur le fond et sur la protection effective des données personnelles dans un espace hors de l'Union Européenne, la Cour précise que « n'est pas limitée au strict nécessaire une réglementation qui autorise de manière généralisée la conservation de l'intégralité des données à caractère personnel de toutes les personnes dont les données ont été transférées depuis l'Union vers les États-Unis sans qu'aucune différenciation, limitation ou exception soit opérée en fonction de l'objectif poursuivi et sans que soit prévu un critère objectif permettant de délimiter l'accès des autorités publiques aux données et leur utilisation ultérieure à des fins précises, strictement restreintes et susceptibles de justifier l'ingérence que comportent tant l'accès que l'utilisation de ces données ».

Dans cet arrêt, la Cour de Justice de l'Union Européenne infirme donc la position de la Commission face au traitement des données personnelles outre Atlantique et fait ainsi tomber le « *Safe Harbor* ».

☛ Avis 1/15 (Accord PNR, Union Européenne-Canada), 26 juillet 2017

En 2014 était signé un accord entre l'Union Européenne et le Canada ayant pour objet le transfert et le traitement des données de dossiers de passagers (accord « PNR »). Le transfert des données s'avérait systématique et continu et concernait l'ensemble des passagers aériens de l'Union Européenne. Le transfert était destiné aux autorités canadiennes et éventuellement à d'autres autorités et pays tiers.

Dans ces données, étaient transférés le nom, les coordonnées du passager mais aussi des informations requises au moment de la réservation (dates du voyage, itinéraire, groupes de personnes

englobées par le même numéro de réservation, informations sur les moyens de paiement et de facturation, bagages etc.).

Le projet était passé du Conseil de l'Union européenne au Parlement qui avait, lui*, demandé à la Cour de Justice de vérifier si l'accord était conforme au droit de l'Union, notamment avec les exigences de respect de la vie privée et de protection des données personnelles*.

Dans cet avis émis en 2017, la Cour a estimé que l'accord ne pouvait pas être conclu en l'état, du fait d'un certain nombre d'incompatibilité entre les dispositions et les droits fondamentaux consacrés par l'Union.

Tout d'abord elle relève que le transfert de ces données constitue une ingérence, à la fois à l'article 7 qui est celui prévoyant le droit au respect de la vie et familiale, qu'à l'article 8 qui consacre la protection des données à caractère personnel.

Elle souligne également que, si prises isolément, certaines données ne semblaient pas dévoiler des informations trop personnelles sur les individus, une fois prises ensemble, elles pouvaient notamment révéler un itinéraire de voyage, la consistance d'un groupe familial ou amical, et même les habitudes ou préférences alimentaires et de santé de certaines personnes.

Dès lors, bien que certaines ingérences trouvent leur justification dans la recherche d'une garantie de sécurité publique en luttant contre les infractions terroristes (objectif d'intérêt général), plusieurs dispositions dépassaient le cadre strictement nécessaire et restaient peu claires et imprécises (notamment le risque d'un traitement contraire au principe de non- discrimination qui nécessiterait alors une justification précise, solide et tirée de motifs graves).

La Cour a également souligné la durée excessive (5 ans) de conservation des données pour des passagers aériens pour lesquels un risque en matière de terrorisme ou de criminalité transnationale grave n'a pas été identifié à leur arrivée au Canada et jusqu'à leur départ de ce pays.

Enfin, la Cour rappelle qu'en matière de traitement de données, l'individu qui y est doit pouvoir s'assurer que ses données personnelles sont traitées de manière exacte et licite. Pour se faire, il doit donc disposer d'un droit d'accès à ses données traitées.

Ainsi, la Cour indique que dans l'accord PNR, les passagers doivent être informées du transfert et de l'utilisation dès lors que cette information ne s'oppose pas à la bonne conduite des enquêtes menées par les autorités publiques.

☛ Arrêt Commission / Facebook Irlande / Schrems, 16 juillet 2020

Faisant suite à la première décision rendue en sa faveur (*Arrêt Schrems, Cour réunie en Grande chambre, 6 octobre 2015)*, Max Schrems, un étudiant autrichien, a une nouvelle fois saisi la justice irlandaise, considérant encore que ses données n'étaient pas en sécurité, malgré le *Privacy Shield* et

les clauses contractuelles types dont il était fait usage entre les pays tiers et l'Union Européenne. Devant la juridiction, il exigeait l'interdiction du transfert de ses données personnelles, de l'UE vers les États-Unis.
A nouveau, une question préjudicielle est adressée à la Cour de justice de l'UE, qui se voit interrogée sur la validité de ces deux dispositifs.

La Cour indique d'abord que dès lors qu'un transfert de données personnelles a lieu dans un but commerciales, et que ces données sont susceptibles d'être traitées à des fins de sécurité publique, de défense et de sûreté par les autorités américaines, il y a nécessairement application du RGPD.
Or, la Cour considère que l'accès et l'utilisation des données personnelles réglementées par les autorités publiques américaines, ne répondent pas aux exigences de protection édictées par le RGPD (pas de limitation au strict nécessaire et donc non-respect du principe de proportionnalité).

Finalement, le *Privacy Shield* est invalidé en raison de son niveau de protection insuffisant.

S'agissant des clauses contractuelles, la Cour pose la nécessité qu'il existe des mécanismes permettant d'assurer que le niveau de protection requis par le RGPD soit bien respecté.
Si de tels mécanismes n'existent pas, les transferts de données personnelles doivent être suspendus voire même interdits.

Sous réserve de cette condition, la Cour de Justice confirme donc la validité des clauses contractuelles, dispositions prévues par la Commission européenne.

4. Autorités nationales de contrôle et portée de leur exigence d'indépendance

☛ Arrêt Commission / Allemagne, Cour réunie en Grande chambre, 9 mars 2010

Dans cette affaire, c'est la Commission Européenne et l'Allemagne qui s'opposaient. La première avait introduit un recours, indiquant que les autorités de protection des données personnelles allemandes faisaient partie intégrante de l'administration régionales, et étaient de fait, soumises au contrôle de l'État. Cette configuration faisait donc obstacle aux exigences d'indépendances posées par la directive 95/46/CE.

Face à cela, la République fédérale d'Allemagne soutenait, elle, que la directive exigeait simplement une indépendance « fonctionnelle » des autorités de contrôle. Ainsi, la tutelle de l'État mise en cause en l'espèce ne constituait pas une influence extérieure, mais un mécanisme de surveillance interne à l'administration.

La Cour a finalement tranché en indiquant que la tutelle de l'État qui était exercée sur les autorités de contrôles du traitement des données personnelles n'était pas compatible avec l'exigence d'indépendance requise par la directive.

Elle formule en effet que « *cette indépendance exclut non seulement toute influence exercée par les organismes contrôlés, mais aussi toute injonction ou toute autre influence extérieure, que cette dernière soit directe ou indirecte* ».

Cet arrêt permet de réaffirmer les exigences de l'Union Européenne quant aux autorités administratives indépendantes.

☛ **Arrêt Commission / Hongrie, Cour réunie en Grande chambre, 8 avril 2014**

Constatant que la Hongrie avait mis fin au mandat de son autorité nationale de contrôle de la protection des données personnelles de manière anticipée, la Commission avait saisi la Cour de Justice afin qu'elle constate un manquement à ses obligations, et ce en vertu de la directive 95/46/CE.

La Cour a effectivement jugé qu'un pays membre de l'Union Européenne qui met fin au mandat de l'autorité de contrôle de la protection des données à caractère personnel ne remplit pas les obligations qui lui incombent en vertu de la directive.

Dans cet arrêt, la Cour rappelle à nouveau la nécessité d'indépendance dont doivent jouir les autorités qui sont compétentes dans la surveillance du traitement des données personnelles. Cela doit donc exclure l'usage d'injonction ou d'influence qui pourraient influer sur les tâches confiées à ces autorités.
Elle rajoute que la possibilité offerte à un État de mettre fin au mandat d'une autorité, de manière anticipée, peut participer à un ressenti de menace, qui pourrait lui-même conduire à une forme d'obéissance, de l'entité au pouvoir politique responsable. Dans ce cas, il s'agirait donc bien d'une incompatibilité avec l'exigence d'indépendance requise.