

Nog te verkrijgen / Encore disponibles:

Dossier 11, 2005, Assurances et droit fiscal
Verzekeringen en fiscaal recht

Dossier 13, 2007, Discrimination, différenciation hommes/femmes et assurances
Discriminatie, geslachtsdifferentiatie en verzekeringen

Dossier 14, 2008, Levensverzekeringen en giften
Assurances Vie et libéralités

Dossier 15, 2009, Solvency II & IFRS

Dossier 16, 2010, De informatieplicht in verzekeringen / Le devoir d'information en assurances

Dossier 17, 2011, Réforme du contrôle du secteur financier (*Twin Peaks*)
Hervorming van het toezicht op de financiële sector (*Twin Peaks*)

Dossier 18, 2012, La compliance en assurance
Compliance in verzekering

www.bulletindesassurances.be
www.tijdschriftvoorverzekeringen.be

De teksten uit dit tijdschrift worden ook online gepubliceerd op Jura en Jura Notariaat.

Les textes de cette revue sont également publiés en ligne sur Jura et Jura Notariat.

Dossier-Tijdschrift voor verzekeringen / Bulletin des assurances

Uitgegeven door:

Kluwer

Édité par:

Kluwer

Verantwoordelijke uitgever:

Hans Suijkerbuijk
Motstraat 30
2800 Mechelen

Éditeur responsable:

Hans Suijkerbuijk
Drève Richelle 161 L
B-1410 Waterloo

Klantenservice Kluwer:

Tel.: 0800 40 300 (gratis oproep)
info@kluwer.be

Service clientèle:

Tél.: 0800-40 330 (appel gratuit)
info@kluwer.be

ISBN: 978-90-46-55889-8

ISBN: 978-90-46-55889-8

© 2014 Wolters Kluwer Belgium NV

Behoudens de uitdrukkelijke bij wet bepaalde uitzonderingen mag niets uit deze uitgave veelelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand of openbaar gemaakt worden, op welke wijze ook, zonder de uitdrukkelijke voorafgaande en schriftelijke toestemming van de uitgever.

© 2014 Wolters Kluwer Belgium SA

Hormis les exceptions expressément fixées par la loi, aucun extrait de cette publication ne peut être reproduit, introduit dans un fichier de données automatisé, ni diffusé, sous quelque forme que ce soit, sans l'autorisation expresse et préalable et écrite de l'éditeur.

INHOUDSTAFEL / TABLE DES MATIERES

L'assurance et les nouvelles technologies en 2013: état des lieux Jean-Christophe André-Dumont	11
Samenvatting	13
Résumé	13
I. Introduction	13
II. Technologies visées	14
1. Phase précontractuelle	14
2. Souscription et déroulement du contrat	14
3. Déclaration et suivi de sinistres	15
III. Remarques et questions soulevées par les nouvelles technologies	16
1. Phase précontractuelle	16
1.1. Question préalable: la fonction de l'application numérique'	16
1.2. Informations éventuellement requises	16
1.3. 'Signature' – Signature électronique	19
2. Souscription et déroulement du contrat	21
2.1. Modification d'éléments relatifs au contrat	21
2.2. 'Interfaces' assureur-preneur	21
3. Déclaration du sinistre	22
IV. Conservation et archivage des données sous forme numérique – Aperçu global de la problématique	23
1. Les besoins pour les assureurs	23
1.1. Finalités poursuivies	23
1.2. Intérêts et limites du numérique	23
2. Particularités de l'archivage pour les entreprises d'assurances	25
3. Contraintes	25
3.1. Contraintes d'ordre légal	25
3.2. Contraintes techniques	29
4. Statut juridique du document digital	31
4.1. De lege lata	31
4.2. De lege ferenda	33
V. Conclusions	35
La conclusion du contrat d'assurance par voie électronique Hervé Jacquemin	37
Samenvatting	39
Résumé	39
Introduction	40
I. Objectifs et champ d'application des règles encadrant la conclusion des contrats d'assurance par voie électronique	41
A. Objectifs des dispositions spécialement adoptées pour encadrer la conclusion des contrats (d'assurance) par voie électronique	42

portuun zijn van de Belgische wetgever om de nieuwe Belgische regels in voege te doen treden, wetende dat die binnen een periode van enkele maanden wellicht ingetrokken moeten worden. De markt van vrouwensdiensten is nog niet matuur en onduidelijkheid over toepasselijke regelgeving komt de rechtszekerheid niet ten goede.

E-commerce et numéro de Registre national: une tension insupportable sur la vie privée? (1)

Thierry Léonard

(1) Mes plus vifs remerciements à mon associé et ami Me Etienne WÉRY, tant pour l'idée à la base de cet article que pour sa précieuse relecture.

SAMENVATTING

De problematiek rond het gebruik van de eID in het kader van de e-commerce is op zijn minst paradoxaal te noemen.

Enerzijds draagt de overheid het gebruik ervan uit gelet op de onmiskenbare voordelen ervan zowel wat betreft de eraan verbonden handtekeningfuncties als de rechtszekerheid die ze meebrengt over de identificatie van de drager. Anderzijds wordt het gebruik ervan afgeremd door de rechtsonzekerheid omtrent het gebruik van het rijksregisternummer dat vrij toegankelijk is op de eID.

De voorwaarde dat voorafgaandelijk de toestemming vereist is van het sectoraal comité van het Rijksregister voor de verwerking van het rijksregisternummer komt er in de praktijk op neer dat het gebruik ervan verboden is voor de privésector, behoudens wettelijke uitzondering, in hoofdzaak wanneer het gebruik een doeleinde van algemeen belang nastreeft. Het arrest van het Hof van beroep van Brussel van 9 mei 2012, dat hierna besproken wordt, bevestigt deze vaststelling.

Deze studie toont aan dat men zich ernstige vragen moet stellen bij de opportuniteit en de wettelijkheid van de toepassing van het systeem van voorafgaande goedkeuring door het sectoraal comité van het Rijksregister voor de verwerking van een rijksregisternummer door de privésector, zonder toegang tot het rijksregister, op basis van de vrije en weloverwogen toestemming van de drager van de eID en mits inachtneming van de wet van 8 december 1992 betreffende de bescherming van de persoonlijke levenssfeer.

RÉSUMÉ

La problématique de l'utilisation de l'eID dans le cadre de l'e-commerce est pour le moins paradoxale.

D'une part, son utilisation est clairement prônée par les autorités, qui vantent sans cesse les vertus tant de ses fonctions de signature que de la sécurité juridique qu'elle implique concernant l'identification du porteur. D'autre part, son utilisation est freinée par l'insécurité juridique qui règne autour de l'utilisation du numéro de Registre national, laissé en accès libre sur l'eID.

La condition de l'obtention d'une autorisation préalable du comité sectoriel du Registre national pour tout traitement du numéro de Registre national revient, en réalité, à interdire cette utilisation par le secteur privé, hors exception légale, principalement lorsque cette utilisation poursuit une finalité d'intérêt général. L'arrêt de la Cour d'appel de Bruxelles du 9 mai 2012, commenté ci-après, confirme cette constatation.

La présente étude montre que l'on peut sérieusement s'interroger sur l'opportunité et la légalité de l'application du système d'autorisation préalable par le comité sectoriel à un traitement du numéro de Registre national par le secteur privé, sans accès au Registre national, sur la base du consentement libre et éclairé du porteur de l'eID et dans le respect de la loi du 8 décembre 1992 sur la protection de la vie privée.

1. **L'internet et la collecte de données: généralités.** La relation de commerce électronique permet de récolter un nombre important de données concernant les internautes. Soit que ces informations sont nécessaires en vue de prêter un service offert sur la toile, soit qu'elles révèlent le comportement de ceux-ci. Ces informations permettent de donner accès à des offres publicitaires futures, celles-ci représentant une source de revenus importante pour les prestataires de services de l'information. Elles peuvent également être mises à disposition de tiers dans un marché de données personnelles de plus en plus florissant.

Se pose alors la difficile question du respect des règles relatives à la protection des données. Le régime général se trouve contenu dans la loi du 8 décembre 1992 (ci-après, la 'loi'). Dans la gamme des moyens de protection des données, le recours au consentement est souvent conçu et perçu comme une des garanties les plus élevées de la protection des droits de la personne. C'est pourquoi on le retrouve au cœur de la plupart des règles de protection des données. Tant au niveau des règles de droit commun que de celles spécifiques à la collecte de données à des fins plus commerciales, tel le marketing direct.

Le droit commun de la protection des données confirme le rôle de garantie confié au consentement de la personne à trois niveaux: celui de la légitimation des finalités du traitement, celui de la levée de l'interdiction des données dites sensibles et celui de la levée de l'interdiction des flux transfrontières de données hors de l'UE.

Le consentement permet, en effet, de légitimer la finalité d'utilisation de tout traitement de données en application de l'article 5 de la loi. Toute finalité d'utilisation de données doit, en effet, se fonder sur une des justifications visées par cette disposition. Le consentement de la personne constitue la première cause de légitimation des traitements. Le consentement, alors écrit, permet aussi de lever la plupart des interdictions de traitement de données sensibles prévues par les articles 6 à 8 de la loi. Il permet également de lever l'interdiction d'un flux transfrontière de données (article 22 de la loi). On le retrouve, en outre, au cœur des mesures prises spécifiquement en matière de publicité et de marketing direct. Pensons, par exemple, au régime le l'opt-in des cookies, ou à celui imposé en cas de traitement d'adresses emails à des fins de publicité.

Le consentement de la personne apparaît dès lors, comme en matière de droit commun des droits de la personnalité, comme une condition nécessaire, mais aussi suffisante de traitement de données considérées comme particulièrement attentatoires à la vie privée des personnes concernées. Pour éviter que cette protection devienne illusoire, le consentement doit être la manifestation d'une volonté libre, spécifique et informée. La personne doit savoir exactement ce à quoi elle consent et doit donc être informée du but d'utilisation et des caractéristiques essentielles du traitement. Ce consentement ne doit pas être obtenu sous pression ou en exécution d'une situation de soumission de la personne concernée au responsable du traitement.

2. **L'obtention d'autorisations préalables de comités sectoriels comme condition de licéité des traitements.** Dans certaines hypothèses, le consentement de la personne en vue de collecter ses données dans une relation d'e-commerce ne suffira pas.

On sait que, en Belgique, la possibilité d'obtenir et de traiter certaines données est soumise à l'autorisation préalable de comités sectoriels, autorités hybrides émanant de la Commission de la protection de la vie privée. Il s'agit généralement d'obtenir la communication de certaines données dont le traitement originnaire est opéré par le secteur public en vue de la réalisation de finalités d'intérêt général (2). Ainsi en est-il du comité sectoriel pour l'autorité fédérale chargée d'autoriser toute communication électronique de données personnelles par un service fédéral ou un organisme public avec personnalité juridique (3), du comité sectoriel de la Banque-carrefour de la Sécurité sociale autorisant principalement les communications de données sociales par la Banque-carrefour de la Sécurité sociale (4), le comité sectoriel de la Banque-carrefour des Entreprises qui autorise l'accès à certaines informations détenues par la Banque-Carrefour des Entreprises (5), etc.

Le régime juridique de l'intervention de ces comités n'est pas toujours clair. La plupart du temps, ces comités se voient attribuer une compétence d'autorisation des traitements au contrôle desquels ils sont institués. Cette compétence d'autorisation est dérogoire au droit commun de la protection des données, puisque la Commission de la protection de la vie privée est, en règle, dépourvue de ce type de compétence et reste conçue principalement comme une autorité d'avis en la matière. Le système a été très justement critiqué dès lors que en tant qu'émanation du pouvoir législatif, les décisions de tels comités ne sont pas susceptibles de faire l'objet d'un recours par l'entité qui l'a saisi, ce qui paraît pour le moins aberrant à l'égard d'autorités de protection des droits et libertés des citoyens (6).

Le comité sectoriel du Registre national est amené à jouer un rôle, le cas échéant, essentiel, lors de l'utilisation de l'eID comme moyen d'identification de l'internaute auprès d'un prestataire en ligne. En effet, l'article 8 de la loi du 8 août 1983 impose que toute utilisation du numéro de Registre national, présent sur l'eID, soit soumise à une autorisation préalable du comité sectoriel du Registre national. Or, ce numéro présente, le cas échéant, une grande utilité en vue de jouer le rôle d'identifiant unique dans la banque de données du prestataire. Il permet aussi de jouer le rôle d'une clé de recherche particulièrement sûre.

3. **Objet et plan de la présente contribution.** L'objet de la présente contribution sera d'abord de rappeler le contexte général de l'eID et de son lien avec le Registre national (section 1).

On commentera ensuite les règles d'utilisation des informations contenues dans l'eID en vue de leur traitement par le secteur privé (section 2).

- (2) Mais pas toujours. Ainsi, le comité sectoriel de la santé est, en règle, chargé d'accorder une autorisation pour toute communication de données relatives à la santé au sens de la loi du 8 décembre 1992, que les données aient été collectées par des personnes privées ou publiques (cf. l'article 42, § 2, 3°, de la loi du 13 décembre 2006 portant dispositions diverses en matière de santé).
- (3) Article 36bis de la loi du 8 décembre 1992.
- (4) Article 46, 6°, de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la Sécurité sociale.
- (5) Article 18 de la loi du 16 janvier 20013 portant création d'une Banque-Carrefour des Entreprises.
- (6) Pour une explication et une critique de ce régime, voy. E. DEGRAVE, 'La carte d'identité électronique utilisée comme carte de fidélité: un traitement de données à caractère personnel illégal sanctionné par la Cour d'appel de Bruxelles', note sous Bruxelles (9^e ch.), 9 mai 2012, *J.T.*, 2012, p. 693.

On montrera alors que l'exigence de cette autorisation s'oppose à l'effet légitime du consentement de la personne, qui normalement permet de traiter des données – même sensibles – en vue d'une finalité commerciale (section 3). On se posera la question de savoir si cette exigence supplémentaire s'impose en cas de légitimation du traitement du numéro de Registre national par le consentement du porteur de l'eID et si elle est conforme aux principes de protection des données tels qu'ils sont inscrits dans la Directive générale 95/48 du 24 octobre 1995, implémentée en droit belge par la loi du 8 décembre 1992, telle que modifiée par la loi du 11 décembre 1998.

Section 1. eID et Registre national: le contexte général

4. L'eID et le Registre national. Chaque résident en Belgique est enregistré dans le Registre national, lui-même alimenté par les Registres de population des communes. Toute personne ayant une résidence principale sur le territoire d'une commune belge est, en effet, tenue de s'inscrire sur les Registres de population de celle-ci. La commune transmet d'office au Registre national les informations visées à l'article 3 de la loi du 8 août 1983 organisant un Registre national des personnes physiques. Les Belges reçoivent alors une carte d'identité délivrée par la commune, qui vaut certificat d'inscription dans ses Registres de population (7).

Les informations inscrites sur la carte d'identité présentent, dès lors, une fiabilité et une mise à jour maximale, les personnes étant obligées de s'inscrire et de présenter leur carte d'identité en vue de leur identification par les autorités publiques, cette présentation conditionnant elle-même de nombreuses prestations de service public.

Le Registre national est lui-même rendu accessible aux autres autorités publiques belges ainsi qu'à des organismes privés ou publics de droit belge chargés de tâches d'intérêt général par ou en vertu d'une loi, ainsi que d'autres organismes visés par l'article 5 de la loi du 8 août 1983. Intervient ainsi le comité sectoriel du Registre national, chargé d'autoriser de tels accès. Il vérifie la légalité de l'accès au regard tant de la loi sur le Registre national que de la loi du 8 décembre 1992. Il contrôle, dès lors, les finalités d'utilisation annoncées et le caractère adéquat, pertinent et non excessif des données auxquelles l'accès est demandé.

En 2004, l'Etat belge a investi massivement dans un système de carte d'identité électronique (eID). L'implémentation du système et la distribution des cartes eID ont duré cinq ans.

La carte d'identité comprend diverses données relatives à l'identification de la personne qui sont visibles à l'œil nu ou de manière électronique (8). Une de ces informations est le numéro d'identification du Registre national, numéro unique attribué à chaque personne inscrite au Registre. La résidence principale et les informations

(7) Article 6, alinéa 1^{er}, de la loi du 19 juillet 1991 relative aux Registres de population, aux cartes d'identité, aux cartes d'étranger et aux documents de séjour.

(8) Le nom, les deux premiers prénoms, la première lettre du troisième prénom, la nationalité, le lieu et la date de naissance, le sexe, le lieu de la délivrance de la carte, la date et le début de la fin de la délivrance de la carte, la dénomination et le numéro de la carte, la photographie du titulaire et le numéro d'identification du Registre national (cf. article 6, § 2, de la loi du 19 juillet 1991 relative aux Registres de population, aux cartes d'identité, aux cartes d'étranger et aux documents de séjour).

relatives au système de signature électronique inclus dans la carte ne sont lisibles que de manière électronique.

Certaines de ces informations peuvent être utiles – voire nécessaires – tant pour s'assurer de l'identité du consommateur que pour mettre à jour les données concernant la personne, sans parler de la fonction de signature qui peut trouver de multiples applications dans l'environnement numérique (signature d'emails ou de documents ou formulaires transmis en ligne). Cependant, mis à part les cas prévus par la loi, la personne reste libre de (ne pas) présenter et/ou d'utiliser ou non sa carte eID dans ses relations avec un prestataire de services public ou privé.

5. L'eID et le commerce électronique. On se souviendra que la carte eID a été présentée comme un outil d'identification, d'authentification et de signature, censé non seulement servir de socle à l'e-gouvernement, mais aussi favoriser le développement du commerce électronique en Belgique (9).

Près de dix ans après sa création, force est de constater que le succès du système est mitigé: si certaines applications commencent à être fréquemment utilisées dans la relation entre personnes privées et autorités publiques, les applications dans le secteur privé sont rarissimes (10).

L'obligation pour l'internaute de se munir d'un lecteur de carte, de télécharger le logiciel eID et l'utilisation de la fonction d'authentification pour accéder à l'application sont autant d'obstacles à l'utilisation de la carte électronique. Du reste, l'utilisation de plus en plus généralisée des smartphones et tablettes pose difficulté, ceux-ci étant le plus souvent dépourvus de ports USB permettant seuls la connexion du lecteur de carte. Les prestataires privés préfèrent, dès lors, opter pour des solutions d'identification plus rapides même si moins sûres. A l'heure actuelle, un ménage sur trois seulement dispose d'un lecteur de carte (11).

A ces difficultés inhérentes à l'utilisation de la carte d'identité électronique s'ajoute la problématique de l'utilisation du numéro d'identification du Registre national,

(9) Et donc de favoriser son utilisation par le secteur privé. Voy., par exemple, l'espoir suscité par le fait que le site eBay Belgique permettait un enregistrement via la carte et l'application eID dans eID Newsletter n° 8 ? Juin 2008 (disponible sur www.ibz.rm.fgov.be). Aussi, E. WERY, 'Première mondiale: le site belge eBay utilise la carte d'identité électronique pour authentifier les utilisateurs', actualité du 28 février 2008, accessible sur www.droit-technologie.org. Voy. aussi la manière dont le SPF Economie présente les potentialités de l'eID pour le commerce électronique dans une étude parue en 2008: *Etude prospective sur les potentialités économiques liées à l'utilisation de la carte d'identité électronique et de la signature électronique* disponible sur <http://economie.fgov.be>; voy. également la politique de développement des applications eID pour tous secteurs prônée par la Fedict sur <http://eid.belgium.be>.

(10) Il est difficile d'obtenir des chiffres globaux et fiables concernant l'utilisation de l'eID. Selon un audit de la Cour des comptes, le 1^{er} mai 2012, un compteur *ad hoc* relevait 475 applications, réparties entre 234 applications publiques (91 au niveau national, 24 au niveau régional et 119 au niveau local), 208 applications pour entreprises et organismes (106 au niveau national, 29 au niveau régional et 73 au niveau local), 19 applications pour associations et 14 pour et par des citoyens (*La carte d'identité électronique (eID). Clé d'accès du citoyen à l'e-gouvernement*, Rapport de la Cour des comptes transmis à la Chambre des représentants, Bruxelles, novembre 2012, p. 40, disponible sur www.courdescomptes.be/docs/2012).

(11) Selon les données et explications indiquées dans le baromètre de la société de l'information (2013), pp. 32 et 33, disponible sur le site du SPF Economie.

présent sur la carte. L'utilisation de ce numéro – par exemple, comme clé d'identification – est soumise à l'autorisation préalable du comité sectoriel au bénéfice des seules personnes visées par l'article 5 de la loi du 8 août 1983 (12). Récemment, la Cour des comptes présentait l'insécurité juridique liée à la présence du numéro de Registre national sur l'eID comme un frein réel au développement de son utilisation, spécialement dans le secteur privé (13). Elle relevait fort à propos, le regrettable, que: *'Sur le plan légal, une demande n'a de chance d'aboutir que si elle est motivée par l'exécution d'une tâche d'intérêt général. Un usage à des fins purement commerciales est donc exclu'* (14).

Il faut, du reste, rappeler une particularité technique du système qui rend potentiellement illégale toute utilisation de la carte eID par le secteur privé: le prestataire de service aura toujours accès au numéro de Registre national s'il propose à l'internaute de s'identifier avec celle-ci, dès lors que toute application eID est capable de lire le numéro au moment où la carte est insérée dans le lecteur. Même si en réalité, le prestataire ne fait – ni ne compte – faire aucune utilisation spécifique du numéro, il s'agit néanmoins d'un traitement de la donnée qui pourrait être considéré comme illégal sans autorisation préalable du comité sectoriel.

Ce dernier problème, très spécifique, pourrait être réglé dès lors que la loi du 19 juillet 1991 relative notamment aux cartes d'identité prévoit expressément, en son article 6, § 4, qu'un arrêté royal soit pris concernant les contrôles automatisés et que ce dernier pourrait parfaitement prévoir que des systèmes qui ne font rien d'autre que lire le numéro de Registre sans le saisir, soient admis sans passage préalable par le Comité sectoriel (15). On attend cet arrêté depuis près de 11 ans...

Section 2. Règles d'utilisation des données issues de l'eID par le secteur privé, en dehors de l'accès au Registre national

6. La collecte des données de l'eID auprès de la personne elle-même. Une difficulté spécifique se pose, en outre, lorsque le responsable du traitement n'obtient pas les données par un accès au Registre, mais de la personne concernée elle-même. Peut-il librement utiliser et traiter les données issues de la carte d'identité de ses clients?

A priori, la réponse est positive. La carte d'identité est d'ailleurs utilisée journalièrement par la personne afin de s'identifier dans ses relations sociales ou professionnelles (à la réception d'un hôtel, lors de la remise d'un courrier ou d'un colis par des services postaux, lors du retrait d'un titre de transport, etc.). En ce sens, la carte d'identité n'est qu'un support/outil de transmission d'informations et d'identification.

(12) L'article 8 de la loi du 8 août 1983 est rédigé comme suit: *'L'autorisation d'utiliser le numéro d'identification du Registre national est octroyée par le comité sectoriel du Registre national visé à l'article 15, aux autorités, aux organismes et aux personnes visés à l'article 5, alinéa 1er. Le comité sectoriel envoie dans les trente jours après sa décision une copie de celle-ci au ministre de l'Intérieur et au ministre de la Justice. (...)'*

(13) *La carte d'identité électronique (eID). Clé d'accès du citoyen à l'e-gouvernement*, Rapport de la Cour des comptes transmis à la Chambre des représentants, Bruxelles, novembre 2012, p. 43 et s., disponible sur www.courdescomptes.be/docs/2012.

(14) *Idem*, p. 44.

(15) *Idem*, p. 46.

tion que s'approprie chaque titulaire, spécialement contrôlées et validées par les autorités communales qui gèrent les Registres de population.

Aucune règle n'interdit a priori l'utilisation de la carte d'identité dans les rapports privés. Les règles applicables ne sont plus alors celles spécifiques à l'utilisation de la carte dans le rapport avec les autorités publiques (16) – par exemple, celles relatives aux contrôles d'identité par les services de police ou l'identification obligatoire par l'eID auprès des institutions de la sécurité sociale –, mais bien les règles de droit commun.

Ces règles ne portent pas a priori sur l'utilisation de la carte en tant que telle, mais sont relatives aux informations collectées et traitées au départ de l'eID. Rien n'interdit a priori le traitement des données contenues sur la carte, dans le respect des règles de protection des données, essentiellement la loi du 8 décembre 1992.

Cette constatation a été explicitement confirmée par la Commission de la protection de la vie privée dans une recommandation du 25 mai 2011 (17). Elle y applique les règles générales issues du principe de finalité inscrit aux articles 4 et 5 de la loi du 8 décembre 1992. En cas d'application dans le secteur privé, l'identification doit d'abord être nécessaire au service presté. C'est le cas lorsque cette identification est imposée par une loi particulière dans le rapport avec le client ou si cette nécessité ressort du service presté. Ainsi, la Commission souligne que le gérant d'une vidéothèque peut légitimement identifier la personne à laquelle il loue un DVD pour lui établir une carte de membre, afin de pouvoir lui réclamer le bien loué qui n'aurait pas été rapporté (18). Elle admet aussi ce besoin d'identification lors de l'adhésion à un système de fidélisation du client si les avantages liés sont personnels à celui-ci (19).

Partant, la Commission admet aussi la collecte des données pertinentes sur l'eID en cas de lecture électronique, dans la mesure strictement nécessaire au traitement poursuivi (par exemple, le nom, les prénoms et la date de naissance pour une inscription dans un registre de visiteurs) (20).

Le consentement libre et éclairé de l'internaute permet, dès lors, de légitimer le traitement et les données de la carte peuvent être utilisées si elles s'avèrent pertinentes, adéquates et non excessives au regard de la finalité poursuivie. La Commission applique le principe au cas où la carte d'identité est utilisée comme carte de fidélité (21). Elle vise le cas où la lecture de l'eID est opérée en l'absence d'une carte de fidélité spécifique afin d'enregistrer le nombre d'achats en vue d'accorder une réduction ou un avantage quelconque eu égard à leur fidélité. Elle ajoute que, selon

(16) Cf. l'article 1^{er}, al. 2, de l'arrêté royal du 25 mars 2003 relatif aux cartes d'identité: *'L'un ou l'autre de ces documents doit être présenté à toute réquisition de la police, ainsi qu'à l'occasion de toute déclaration, de toute demande de certificats et, d'une manière générale, lorsqu'il s'agit d'établir l'identité du porteur'*.

(17) Recommandation d'initiative de la Commission de la protection de la vie privée du 25 mai 2011 relative à la prise de copie des cartes d'identité ainsi qu'à leur utilisation et à leur lecture électronique, que, disponible sur le site www.privacycommission.be.

(18) *Idem*, § 14.

(19) *Idem*, § 17.

(20) *Idem*, § 22.

(21) *Idem*, § 23.

elle, une alternative devrait être laissée à la personne qui ne voudrait pas utiliser sa carte d'identité à cet effet. Seules les données nécessaires peuvent alors être traitées. Elle exclut notamment la photo, la nationalité ou le lieu de naissance.

La Commission n'exclut donc, dans sa recommandation, ni une utilisation commerciale des données issues de l'eID, ni une utilisation pour une finalité de marketing direct. Même si la mise en œuvre de telles finalités d'utilisation de l'eID sont mises en doute (22), il nous paraît qu'aucune utilisation privée de l'eID n'est exclue par la loi du 25 mars 2003 en vue d'organiser la généralisation de l'eID (23). De plus, la fonction première et principale de l'eID, explicitement attribuée en vertu de la loi par l'article 1^{er} de l'arrêté royal du 25 mars 2003 relatif aux cartes d'identité, est d'établir l'identité de la personne, les données électroniques y contenues devant toutes concourir à cette identification. Cette fonction d'identification est précisément celle utilisée dans le cadre des finalités d'utilisations commerciales dont on parle ici.

Le document est donc utilisé par la personne conformément à la finalité qui lui a été attribuée par ou en vertu de la loi, qui ne se prononce pas – et n'a pas à le faire – sur la légitimité des traitements subséquents d'utilisation, ces derniers étant soumis à la législation sur la protection des données. Enfin, l'assertion contredit les propos tenus par le Roi lors de l'élaboration de l'arrêté royal du 25 mars 2003 (*cf. infra*) et les efforts de l'administration pour favoriser l'utilisation de la carte avec les prestataires privés.

Cette admission du traitement des données accessibles sur l'eID par le secteur privé n'est cependant pas prévue explicitement par la réglementation applicable à la carte d'identité. Toutefois, le rapport au Roi qui précède l'arrêté royal du 25 mars 2003 relatif aux cartes d'identité, confirme le principe d'utilisation de l'eID dans les rapports privés non seulement concernant les fonctions d'authentification et de signature de la carte, mais aussi concernant la lecture et la copie des données d'identification, ce qui ne change rien par rapport aux usages privés de l'ancienne carte (notamment sa photocopie éventuelle dans ce cadre) (24).

Mais le principe vaut-il également pour l'utilisation du numéro de Registre national, dont le caractère unique peut être particulièrement utile comme identifiant dans une banque de données privée de type commercial?

7. La problématique de l'utilisation du numéro de Registre national à des fins privées. Il faut d'emblée distinguer deux situations d'utilisation du numéro de Registre national par le secteur privé.

(22) E. DEGRAVE, 'La carte d'identité électronique utilisée comme carte de fidélité: un traitement de données à caractère personnel illégal sanctionné par la Cour d'appel de Bruxelles', note sous Bruxelles (9^e ch.), 9 mai 2012, *J.T.*, 2012, p. 692. Outre une violation du principe de transparence propre à l'espèce concernant la description de la finalité par le responsable, l'auteur allègue une potentielle contrariété avec la loi du 19 juillet 1991 relative aux Registres de population, aux cartes d'identité, aux cartes d'étrangers et aux cartes de séjour, cette dernière ne permettant pas l'utilisation commerciale de la carte, en tant que document administratif.

(23) L'identification est d'ailleurs la fonctionnalité principale des Registres de population, dont la carte d'identité certifie l'inscription.

(24) Rapport au Roi précédant l'arrêté royal du 25 mars relatif aux cartes d'identité, *M.B.*, 28 mars 2003, spéc. pp. 15930 et 15931.

Soit l'entité privée veut accéder au Registre et utiliser dans ce cadre le numéro de Registre national. Elle est alors soumise – comme les autorités publiques – aux règles spécifiques qui en régissent l'accès. Le traitement se situe dans le cadre du système d'accès et d'échanges d'informations du Registre national. Il va de soi qu'elle ne peut utiliser le numéro pour une autre finalité que celle spécifiquement autorisée par le comité sectoriel (25). Or, une finalité commerciale ou de marketing subéquente ne pourra être permise, ne remplissant pas la condition de tâche d'intérêt général exigée par la loi.

Soit l'entité privée ne veut pas accéder au Registre national et son traitement se situe en dehors du système d'accès et d'échanges de données organisé par le Registre national. L'entreprise, pour des raisons propres, désire néanmoins utiliser le numéro de Registre national et collecte celui-ci auprès du titulaire de l'eID. Dans cette hypothèse, outre le problème de l'application et de l'interprétation des textes relatifs à l'organisation du Registre national, se pose aussi, plus fondamentalement, la question du statut de l'information en cause.

Le numéro de Registre national est une information outil créée par et pour le secteur public, octroyé par l'Etat au citoyen en vue de lui imposer sa transmission et son utilisation dans certaines situations réglementées. Partant de ce constat, on pourrait considérer que le citoyen ne peut en disposer à sa guise, en dehors des cas autorisés ou imposés par l'autorité publique. Néanmoins, dès lors que cette information est incluse dans les informations librement accessibles de la carte eID et qu'elle ne fait l'objet d'aucune protection ou réservation technique aux autorités publiques autorisées, on peut aussi considérer que, en tant qu'information identifiante, elle pourrait être librement utilisée par le titulaire de la carte, protégée – comme toute donnée à caractère personnel – par les règles de protection des données à caractère personnel.

La question de l'utilisation privée des numéros d'identification se pose depuis longtemps. Avant même l'harmonisation européenne des règles de protection des données, on considérait généralement qu'à défaut de base légale spécifique à la communication, les numéros d'identification universels – ou à usages multiples – tel le numéro de Registre national, ne pouvaient être utilisés par le secteur privé qu'avec le consentement de la personne concernée et pour autant que le refus ne génère pas des conséquences négatives, telle l'absence d'accès au service (26).

8. La décision Fidel ID du 9 mai 2012. Une décision récente de la Cour d'appel de Bruxelles (27) tend à donner raison à une interprétation interdisant toute utilisation commerciale du numéro de Registre national par le secteur privé, même si elle ne se pose pas la question en ces termes.

(25) L'article 8, § 2, second al., de la loi du 8 août 1983 organisant un Registre national des personnes physiques le prévoit d'ailleurs explicitement.

(26) *Les numéros personnels d'identification: leur mise en œuvre, leur utilisation et la protection des données*, Conseil de l'Europe, 1991, p. 31, disponible sur le site du Conseil de l'Europe (www.coe.int). Le rapport propose d'ailleurs que le principe soit prévu explicitement dans les législations nationales spécifiques aux numéros d'identification. Voy. aussi les exemples cités de législations nationales implémentant ce type de solution.

(27) Bruxelles (9^e ch.), 9 mai 2012, *J.T.*, 2012, p. 690 et s. et note E. DEGRAVE qui approuve le raisonnement de la Cour.

La société Fidel ID a développé une carte de fidélité basée sur l'utilisation de la carte d'identité électronique en lieu et place des traditionnelles cartes de fidélité. Les commerçants qui utilisent ce système, lisent la carte d'identité électronique des clients au lieu d'une carte de fidélité. Ils sont reliés à une plate-forme qui gère la mise à jour des données en ligne, notamment l'état des programmes de fidélité auxquels participe chaque consommateur. Le numéro de Registre national auquel on accède nécessairement en cas de lecture des données contenues dans la carte d'identité, est codé et utilisé comme identifiant unique des consommateurs.

Le comité sectoriel du Registre national, saisi par la société, avait rendu un avis négatif le 16 février 2011, dans les termes suivants: *'L'autorisation d'accéder aux informations visées à l'article 3, premier et deuxième alinéas de la loi sur le Registre national, ou d'en obtenir communication, et d'utiliser le numéro d'identification du Registre national, peut être accordée par le comité aux organismes publics ou privés de droit belge pour les informations nécessaires à l'accomplissement de tâches d'intérêt général qui leur sont confiées par ou en vertu d'une loi, d'un décret ou d'une ordonnance ou de tâches reconnues explicitement comme telles par le comité sectoriel précité (article 5, alinéa 1^{er}, 2^o, de la loi). Le comité considère par ailleurs que la finalité poursuivie par le demandeur ne peut en aucun cas être assimilée à une mission d'intérêt général. (...) Au vu de ce qui précède la demande n'est pas recevable'*.

Fidel ID passe outre et commercialise son système. Un concurrent décide de le citer en justice en lui reprochant la commission d'un acte contraire aux usages honnêtes en matière commerciale, au sens de la loi sur les pratiques du commerce.

Après avoir reproduit *in extenso* l'article 5 de la loi sur le Registre national et l'avis du comité sectoriel, la Cour d'appel se réfère à la décision dudit comité et conclut: *'qu'il se déduit de ce qui précède qu'à défaut d'autorisation du comité sectoriel du Registre national, Fidel ID utilise le numéro de Registre national repris sur la carte d'identité électronique en violation de la loi'*.

La Cour pousse le raisonnement plus loin: *'en l'état actuel de la législation et à défaut d'une autre technologie, l'utilisation de la carte d'identité électronique des consommateurs comme carte de fidélité commerciale unique est illégale, puisqu'elle permet l'utilisation du numéro de Registre national'*. Elle précise aussi que le fait de crypter ce numéro ne change rien à son constat.

Elle se situe dès lors dans la droite ligne de la recommandation précitée de la Commission de la protection de la vie privée du 25 mai 2011, qui affirme le principe de manière générale comme dans le cas de l'utilisation de la carte eID en tant que carte de fidélité (28).

Rappelant ensuite une jurisprudence aujourd'hui classique, la Cour dit que *'la violation d'une disposition légale qui n'est pas spécialement énumérée par la loi sur les pratiques du commerce peut constituer un acte contraire aux usages honnêtes au sens de cette loi, lorsqu'il est porté atteinte aux intérêts professionnels d'un autre vendeur'*. Tel est le cas lorsque la violation de cette norme crée un avantage compé-

(28) Recommandation d'initiative de la Commission de la protection de la vie privée du 25 mai 2011 relative à la prise de copie des cartes d'identité ainsi qu'à leur utilisation et à leur lecture électronique, disponible sur le site www.privacycommission.be, § 22 et § 23.

titif dans le chef de celui qui commet l'infraction ou, à l'inverse, place ses concurrents dans une situation concurrentielle défavorable.

Dans le cas d'espèce, la Cour estime que *'l'utilisation du numéro du Registre national repris sur la carte d'identité électronique permet d'éviter des investissements importants que devrait consentir toute autre entreprise respectueuse de la loi pour concevoir, fabriquer et gérer une carte à puce susceptible de prodiguer les mêmes avantages économiques que le système Fidel ID'*.

Au niveau des sanctions, la Cour ordonne la cessation immédiate de l'utilisation du numéro de Registre national, mais elle laisse un délai de 30 jours avant de faire cesser les astreintes pour *'tenir compte des difficultés éventuelles que Fidel ID pourrait rencontrer avec les commerçants pour exécuter l'arrêt'*.

9. Intérêt de la décision Fidel ID. Cette décision est intéressante à divers égards.

D'abord, elle rappelle que l'absence d'autorisation d'un comité sectoriel, lorsqu'elle est prévue par la loi, fait courir un risque certain à l'entreprise qui l'a omise ou qui ne s'est pas conformée au rejet de l'autorisation. Le danger ne provient pas seulement des autorités de contrôle, mais bien des concurrents qui voient dans le non-respect de la réglementation spécifique un acte contraire aux pratiques honnêtes du marché. La cessation de l'acte illicite - l'utilisation de la donnée sans autorisation - procure alors une sanction plus efficace que celles - largement inappliquées - des législations sur la protection des données.

Elle met aussi en exergue certaines difficultés d'interprétation de ces législations protectrices dérogatoires au droit commun. En effet, dans le cas soumis à la Cour, il ne s'agissait pas d'obtenir un accès au numéro de Registre national via le Registre lui-même, pour un nombre a priori illimité de personnes. L'utilisation de la donnée pouvait se prévaloir a priori du consentement préalable de chaque utilisateur du service.

Se pose aussi la question de la pertinence et de la conformité au droit européen de l'autorisation préalable exigée par la législation sur le Registre national.

Section 3. La controverse: consentement de la personne vs. autorisation du comité sectoriel

10. L'insuffisance du consentement de la personne pour traiter le numéro de Registre national? En droit commun de la protection de la vie privée, le consentement libre et éclairé est seul capable de couvrir les intrusions les plus profondes dans l'intimité de la personne. Il révèle le pouvoir de contrôle et la maîtrise de la personne elle-même sur les biens de sa personnalité. Il lui revient de décider, en connaissance de cause, ce qu'il lui plaît de révéler ou non. Le régime des données sensibles, rappelé ci-avant y fait écho: le consentement de la personne lève normalement l'interdiction de principe au traitement.

Si on suit l'interprétation retenue par la Cour d'appel, en l'absence d'une autorisation préalable du comité sectoriel, le consentement de l'individu ne suffit pas pour permettre la communication et le traitement du numéro d'identification.

Nous parlons bien ici du numéro de Registre national, et non du Registre national en tant que base de données. Le Registre national est, en effet, une base de données

centralisant pour chaque citoyen les données que la loi prévoit (29). Au sein de cette base de données, chaque citoyen est identifié par un numéro d'ordre unique, appelé 'numéro de Registre national'. Ce numéro – qui est un numéro d'ordre – ne doit donc pas être confondu avec les informations matérielles contenues dans le Registre national. Sauf à avoir accès au Registre national – ce qui n'est pas l'objet de notre étude et fait l'objet d'un contrôle strict via le comité sectoriel (voir *supra*) – ce numéro doit être pris pour ce qu'il est: un numéro d'ordre qui présente la particularité d'être (i) unique pour chaque personne, et (ii) fiable.

Ce numéro d'ordre figure sur la puce de la carte d'identité électronique. Lorsqu'elle est lue et que le citoyen tape son code, il fait donc partie des données d'identification fournies volontairement par le citoyen. Tel est bien l'enjeu de notre étude.

11. Les finalités du numéro de Registre national. Le numéro d'identification du Registre national n'est certes pas une information classique. Il faut bien comprendre pourquoi il a été créé et, partant, les risques qui y sont liés en termes de traitement.

Il faut d'abord souligner l'origine 'publique' du numéro d'identification du Registre national qui n'est, au départ, qu'un numéro d'inscription au Registre national organisé par la loi du 8 août 1983 (30). Il s'agit donc d'une information créée par et pour le secteur public dans le cadre de l'organisation du Registre national, voué essentiellement à la facilitation des échanges d'informations entre les administrations et la mise à jour automatique des fichiers du secteur public (31).

En tant que tel, il ne comprend comme données utilisables que la date de naissance et le sexe. C'est en effet principalement une donnée outil pour l'administration: il permet d'identifier la personne/citoyen en réduisant au maximum le risque d'erreur sur la personne. Octroyé au moment de l'enregistrement des autres données dans le Registre national, il permet de garantir que ces autres données se rapportent bien à la personne en cause. De ce fait, il permet aussi de servir d'identifiant unique par toutes les entités publiques qui ont accès au Registre national et, le cas échéant, d'unifier autour de lui les différentes informations détenues par chacune de celles-ci et de contrôler l'exactitude de celles qui sont collectées directement par ces administrations auprès des citoyens. Le numéro de Registre national est d'ailleurs utilisé comme numéro d'identification par la sécurité sociale (NISS) et l'administration fiscale (NIF).

Dans ce système l'eID, en tant qu'elle comprend elle-même le numéro de Registre national, sert de moyen de collecte initial en vue de la vérification de l'identité de son porteur et de l'accès éventuel aux autres données contenues dans le Registre national.

(29) Voir www.droit-technologie.org/actualite-947/la-belgique-etend-considerablement-la-liste-des-informations-figurant.html.

(30) Voy. l'arrêté royal du 3 avril 1984 relatif à la composition du numéro d'identification des personnes inscrites au Registre national des personnes physiques.

(31) L'article 1^{er}, § 2, de la loi du 8 août 1983: 'Le Registre national met à la disposition des autorités, organismes et personnes visés à l'article 5 un fichier national en: a) facilitant l'échange d'informations entre administrations; b) permettant la mise à jour automatique des fichiers du secteur public en ce qui concerne les informations générales sur les citoyens, dans la mesure où la loi, le décret ou l'ordonnance l'autorise; c) rationalisant la gestion communale des Registres de la population; d) simplifiant certaines formalités administratives exigées des citoyens'.

Le numéro de Registre national permet donc de poursuivre au moins deux finalités directement liées dans le système du Registre national: l'identification de la personne et la recherche ou le contrôle d'informations relatives au citoyen.

12. Les risques liés à l'utilisation du numéro de Registre national. L'utilisation et la mise en oeuvre d'un numéro d'identification générale et unique pour l'ensemble de la population d'un Etat a toujours suscité une crainte pour les droits et libertés individuels et, partant, une réticence à son adoption dans les pays démocratiques. C'est que l'utilisation de ces numéros et le débat qui l'accompagne, précèdent l'ère 'informatique' ainsi que les législations protectrices des données. Le débat suscité a d'ailleurs joué un rôle de moteur à l'adoption des premières législations de protection des données à caractère personnel, en Europe (32). En Belgique, le système initial d'octroi du numéro d'identification a été mis en place en 1983, soit neuf ans avant l'adoption de la première loi sur la protection des données.

La finalité d'identification ne paraît pas présenter un danger en elle-même. Elle permet, au contraire, de diminuer le risque d'erreur sur la personne et dès lors, d'éviter la collecte et le traitement d'informations erronées la concernant.

Cette constatation trouve une application significative dans l'arrêté royal du 24 novembre 2010 déterminant les cas dans lesquels une autorisation d'utiliser le numéro d'identification du Registre national n'est pas requise. Celui-ci permet aux organismes et personnes qui ont été autorisés à accéder aux informations du Registre national d'enregistrer en interne le numéro d'identification aux seules fins de consulter le Registre national dans le respect de la finalité autorisée. Comme l'indiquent le rapport au Roi et le comité sectoriel, le but est d'éviter que les institutions consultent des données relatives à des personnes non concernées par la finalité de la consultation, ce que permet d'éviter des recherches ultérieures fondées sur le numéro de Registre national. Evidemment, les autorités en cause ne peuvent faire aucune autre utilisation du numéro.

Par contre, la fonction de clé de recherche du numéro d'identification, permettant de contrôler, de mettre à jour et de rassembler, par rapprochement autour de lui, un grand nombre d'informations sur la même personne alors que ces informations auraient été collectées pour des finalités différentes ou incompatibles par des entités différentes pose une difficulté classique en la matière: une utilisation généralisée du numéro facilite et, le cas échéant, augmente le risque de détournements de finalités, en déjouant les attentes légitimes des personnes concernées quant aux utilisations futures de leurs données dans un système où ils ne maîtrisent pas la collecte et l'utilisation dudit numéro par les pouvoirs publics. Le danger s'accroît dès lors que l'utilisation du numéro d'identification se réalise au départ d'un accès à une banque de données contenant l'intégralité des personnes résidant sur le territoire d'un Etat, comme le Registre national.

Plus fondamentalement, c'est la crainte d'une augmentation du pouvoir de l'administration par une capacité toujours plus grande de traiter les données de citoyens –

(32) Pour un exposé plus complet sur le contexte et la perception de la problématique du traitement des numéros d'identification, voy. *Les numéros personnels d'identification: leur mise en oeuvre, leur utilisation et la protection des données*, Conseil de l'Europe, 1991, disponible sur le site du Conseil de l'Europe (www.coe.int).

et donc de les contrôler – qui alimente la crainte légitime de nos sociétés démocratiques à l'égard des numéros d'identification uniques.

Au-delà des possibilités d'interconnexion qui ne sont pas un risque propre créé par le système, l'accès au Registre national présente en définitive deux risques majeurs : d'une part, il se fait à l'insu de la personne concernée, et d'autre part, il peut en théorie donner lieu à des traitements de masse.

C'est pourquoi, fondamentalement, sans toutefois souscrire à toutes les modalités d'organisation de celui-ci, nous pouvons comprendre la légitimité d'un système d'autorisation préalable des comités sectoriels permettant de filtrer les demandes d'accès au Registre national et de vérifier les utilisations qui pourraient être faites du numéro national par les demandeurs d'accès au Registre, voire d'autres entités n'ayant pas accès au Registre.

13. Les risques spécifiques à l'utilisation commerciale du numéro de Registre national. Est-il cependant opportun et justifié de soumettre toute utilisation du numéro de Registre national à l'autorisation du comité sectoriel dès lors que celui-ci serait directement collecté auprès des consommateurs, sur la base de leur consentement, et qu'elle n'aurait pas pour but de rassembler l'information le concernant au travers des banques de données du secteur public ?

Comme le souligne la Cour des comptes, le numéro d'identification n'est pas une clé d'accès aux banques de données du secteur public, mais une clé de recherche d'informations dans celles-ci (33). Sa 'puissance' est donc principalement fonction de l'ampleur et du nombre de banques de données dans lesquelles il est utilisé comme identifiant. Sa seule connaissance par une entreprise privée, qui n'a nullement accès aux gisements de données du secteur public afin de l'utiliser comme clé de recherche, n'augmente donc pas le pouvoir de celle-ci et, partant, le risque d'interconnexion.

Le véritable problème se situe, par contre, par rapport aux pouvoirs publics eux-mêmes. Ceux-ci pourraient être tentés de forcer un accès aux données du secteur privé voyant leur entreprise facilitée par un emploi généralisé du numéro de Registre national dans les banques de données privées cibles. Comme l'a souligné la Commission de la protection de la vie privée, le risque véritable pour les citoyens consiste dans la possibilité d'interconnecter 'tous les fichiers des organisations privées et publiques' (34). Comme le soulignait un rapport du Conseil de l'Europe, le danger

(33) La carte d'identité électronique (eID). Clé d'accès du citoyen à l'e-gouvernement, Rapport de la Cour des comptes transmis à la Chambre des représentants, Bruxelles, novembre 2012, p. 44, disponible sur www.courdescomptes.be/docs/2012.

(34) Avis de la Commission de la protection de la vie privée n°19/2002 du 10 juin 2002, projet de loi modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques et la loi du 19 juillet 1991 relative aux Registres de la population et aux cartes d'identité et modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques, *Doc. Parl.*, Ch., sess. ord. 2002-2003, n°2226/02, p. 14. Voy. aussi p. 16, § 23 où la Commission se dit opposée à une libéralisation inconditionnelle du numéro de Registre national, en rappelant néanmoins que 'le problème réel soulevé par les identifiants de quelque nature qu'ils soient, n'est pas leur dangerosité en soi mais les interconnexions qu'ils autorisent. C'est le contrôle des interconnexions de fichiers et de leur finalité qui est le véritable enjeu du débat'.

est de voir le pouvoir de contrôle des citoyens par l'administration augmenter encore, par un enrichissement facilité de ses propres données (35).

Ce rapprochement est cependant assez théorique dans nos sociétés démocratiques actuelles, dotées de législations protectrices des citoyens, imposant le respect de leurs droits et libertés fondamentales dans le cadre de l'application stricte du principe de légalité et de proportionnalité aux pouvoirs publics. Le tout sous le contrôle de juridictions internationales, telle la Cour européenne des droits de l'homme. On ajoutera que si l'autorité impose à un secteur ou à certaines entreprises de transférer certaines données qu'elles traitent, le fait même de l'absence d'utilisation du numéro de Registre national n'empêchera pas l'interconnexion imposée. Inversement, l'accès aux données à caractère personnel détenues par le secteur public fait l'objet d'une réglementation stricte, les règles d'accès au Registre national le rappelant, si besoin est.

Du reste, si les dangers liés à une utilisation forcément ponctuelle et circonstancielle du numéro de Registre national par les entreprises privées, dans le cadre des règles générales de protection des données, étaient si grands, pourquoi avoir laissé cette information en accès libre sur l'eID, sachant que la carte serait forcément utilisée par l'individu dans ses relations privées ? La question a été posée durant l'élaboration de la loi du 25 mars 2003. Le projet initial était, en réalité, de libéraliser l'utilisation du numéro de Registre national. La Commission de la protection de la vie privée (36) et le Conseil d'Etat s'y sont opposés, et le gouvernement est revenu sur sa copie. Il a toutefois refusé de retirer le numéro des informations lisibles à l'oeil nu et électroniquement, par souci d'efficacité d'utilisation et de collecte de ce numéro. Il s'est notamment justifié par le fait que le danger réel quant à celui-ci était dans la possibilité de l'utiliser comme clé d'accès au Registre national, danger précisément écarté par les règles *ad hoc* sur l'accès au Registre national contenues dans la loi du 8 août 1983 telle que modifiée (37).

(35) Les numéros personnels d'identification: leur mise en oeuvre, leur utilisation et la protection des données, Conseil de l'Europe, 1991, p. 23, disponible sur le site du Conseil de l'Europe (www.coe.int).

(36) On peut notamment lire dans son avis: 'La Commission, tout en acceptant une position plus libérale que celle restrictive adoptée jusqu'à présent, refuse de considérer cependant le numéro de Registre national comme un simple identifiant comme les autres. Il est évident que ce numéro, dans la mesure où il présente des qualités particulières de fiabilité dans son attribution et pour sa vérification, et où il vise l'ensemble de la population, revêt un caractère obligatoire et surtout permet, si son utilisation est libre, d'interconnecter potentiellement du moins tous les fichiers des organisations privées et publiques, ce qui crée un risque important pour les citoyens' (Avis de la Commission de la protection de la vie privée n°19/2002 du 10 juin 2002, *op. cit.*, p. 14).

(37) Projet de loi modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques et la loi du 19 juillet 1991 relative aux Registres de la population et aux cartes d'identité et modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques, Exposé des motifs, *Doc. Parl.*, Ch., sess. ord. 2002-2003, n°2226/01, pp. 27 et 28, où l'on lit également: 'Le raisonnement du Conseil d'Etat selon lequel par une publicité systématique un risque d'usage abusif du numéro d'identification apparaitrait, pourrait en fait être tiré pour les autres données de la carte d'identité qui sont également publiques. Pourquoi ces données pourraient-elles être publiques et pas la clé d'accès à ces données?' (p. 27).

En outre, comme le souligne la Cour des comptes (38), les progrès techniques et les changements de mentalité liés à l'utilisation des réseaux sociaux forcent à relativiser quelque peu la puissance due au caractère unique de l'identifiant public qu'est le numéro de Registre national. Ainsi, la puissance toujours plus grande des moteurs de recherche sur internet, associée au nombre de plus en plus important d'informations rendues publiques par les personnes elles-mêmes – par exemple, sur les réseaux sociaux qu'ils soient privés ou professionnels – permet une identification de plus en plus certaine des personnes, indépendamment d'un identifiant unique.

Inversement, l'utilisation du numéro de Registre national dans le secteur privé pourrait remplir la même fonction d'identification que dans le secteur public, augmentant également la confiance dans les échanges électroniques privés. Lié à la carte eID et autres informations qu'elle contient, le numéro authentifie la personne et garantit l'exactitude des informations qui y sont liées, pour autant qu'elles puissent être mises à jour. Une meilleure identification n'est pas un risque, mais participe à une meilleure protection des individus. Dans l'univers numérique, elle sécurise les acteurs de l'échange et renforce la sécurité juridique en cas de transmission d'informations ou de conclusion d'un acte juridique.

Certes, une utilisation généralisée de l'identifiant unique qu'est le numéro de Registre national – accessible via l'eID – facilite le rapprochement et la connexion de données entre entités privées et, partant, comme dans le secteur public, celui d'un détournement de finalités. Il ne faut cependant pas se tromper : ce n'est pas la meilleure identification des personnes qui crée le risque de détournement de finalités. Et les moyens d'interconnexion évoluent sans cesse, de sorte que la nécessité même de l'utilisation du numéro de Registre à cette fin ne s'impose plus. Le détournement de finalité doit être combattu et évité par l'application toujours plus efficace des règles de protection des données et par une plus grande responsabilisation des acteurs. Sous peine de disproportion, le traitement du numéro de Registre ne peut être interdit sur la seule raison de l'existence d'un risque de rapprochement des traitements, si l'on se prive ainsi d'éviter au maximum les risques d'erreur sur la personne.

Tenant compte de ces divers éléments, la nécessité de soumettre toute utilisation du numéro de Registre national dans le secteur privé au comité sectoriel, dans les mêmes conditions strictes actuelles d'accès au Registre national, nous paraît de plus en plus douteuse. Si le problème est celui d'une possibilité d'interconnexion des traitements des secteurs privés et publics, comme l'a souligné avec raison la Commission de la protection de la vie privée, ce sont les conditions d'interconnexion entre ces deux catégories de traitements qu'il fallait réglementer. L'interdiction de traiter le numéro d'identification par le secteur privé en dehors de tâches d'intérêt général qui seraient confiées aux entreprises, ne rencontre pas en tant que tel le problème d'interconnexion particulier en cause. Il a, par contre, pour conséquence d'interdire purement et simplement l'utilisation de l'identifiant dans la relation habituelle des entreprises avec les personnes et, on l'a vu, de freiner l'utilisation de l'eID dans une relation de commerce électronique. On perd alors tous les avantages qui y seraient liés tant pour l'entreprise que le client.

(38) La carte d'identité électronique (eID). Clé d'accès du citoyen à l'e-gouvernement, op. cit., p. 14, disponible sur www.courdesscomptes.be/docs/2012.

En toute hypothèse, les règles actuelles du droit commun de la protection des données permettent d'assurer le respect des droits individuels des personnes et de lutter contre les interconnexions indésirables ou présentant des dangers particuliers. Comme l'utilisation du numéro de Registre national paraît un élément de sécurisation et de plus grande efficacité dans les relations entre citoyens et l'administration, voire de protection de la vie privée, on ne voit pas pourquoi une telle utilisation ne pourrait pas, dans le respect de la loi du 8 décembre 1992, être également permise par le secteur privé, dans le seul but d'identification des personnes concernées et sans accès concomitant au Registre national. Il y va d'ailleurs de leur intérêt supérieur à ne pas être confondue avec celui d'un d'autre.

14. Les deux interprétations de l'article 8 de la loi du 8 août 1983. L'interprétation du champ d'application de l'article 8 de la loi du 8 août 1983 admise par la Cour d'appel va à l'encontre des constatations qui précèdent, en confirmant une interprétation stricte des textes existants. Ce faisant, la Cour confirme l'interdiction de toute utilisation du numéro de Registre national par le secteur privé, en dehors de l'exercice d'une tâche d'intérêt général. L'autorisation du comité sectoriel est requise pour toute utilisation du numéro d'identification, liée ou non à une demande d'accès au Registre national ou de communication des données qu'il contient. La Cour, comme le comité sectoriel, fait une application stricte de l'article 8 qui n'impose pas que la demande d'utilisation du numéro de Registre national soit liée à un accès au Registre, pour donner lieu à la procédure d'autorisation (39). On l'a vu, cette disposition est née de l'abandon par le législateur de sa volonté initiale de libérer l'utilisation du numéro de Registre national (40) et de la proposition de la Commission de la protection de la vie privée de conserver la soumission de l'utilisation du numéro de Registre national à certaines conditions, reprises dans le texte final.

Une autre interprétation, restrictive, paraît cependant possible (41).

L'utilisation du numéro de Registre national visée par les dispositions précitées ne vaudrait que dans le cadre du système d'accès et de recherche du Registre national, mis en place par la loi du 8 août 1983. Dans cette vision, les articles 5 et 8 de la loi du 8 août 1983 ont des champs matériels différents, qui se complètent dans le cadre de l'accès au Registre national. L'article 5 réglemente l'accès et la communication des données du Registre national, à l'exception du numéro de Registre national, non visé par les informations mentionnées à l'article 3, qui peuvent seules faire l'objet de la demande. Si un organisme ou une personne susceptible d'accéder au Registre veut utiliser le numéro d'identification généré par l'enregistrement dans le Registre, il peut introduire la demande spécifique de l'article 8. La collecte du numéro se fait

(39) Pour d'autres exemples, voy. Délibération RN n° 21/2012 du 14 mars 2012 du comité sectoriel du Registre national relative à la demande de l'ASBL GOCA et de 8 sociétés agréées pour le contrôle technique des véhicules d'utiliser le numéro d'identification du Registre national dans le cadre de l'organisation des examens pour le permis de conduire, accessible sur www.privacycommission.be; Délibération RN n° 74/2009 du 23 décembre 2009 du comité sectoriel du Registre national relative à l'utilisation du numéro de Registre national des clients résidentiels finals par leurs fournisseurs respectifs d'électricité et de gaz naturel et par les gestionnaires de réseaux de distribution, exclusivement en vue de l'application automatique des prix maximaux sociaux aux clients protégés résidentiels finals, accessible sur www.privacycommission.be.

(40) Cf. *supra*, § 13.

(41) E. WERY, 'Le Registre national de la population belge peut-il être utilisé à des fins commerciales?', actualité du 15 mars 2013, accessible sur www.droit-technologie.org.

alors soit sur la base d'un accès préalable au Registre, soit sur la base de sa collecte directe, considérée comme nécessaire à la tâche d'intérêt général dont est légalement chargé le responsable du traitement.

La finalité d'utilisation du numéro de Registre national se trouve ensuite limitée par les objectifs et finalités attribués au système du Registre national par l'article 1^{er}, § 2, de la loi du 8 août 1983 (42). Le but est de faciliter l'échange d'informations entre administrations et de permettre la mise à jour des fichiers du secteur public. Il n'est pas reconnu par la loi aux données contenues dans le Registre et au système de communication de celles-ci aux tiers, une fonction d'identification des personnes, contrairement à la carte d'identité (43).

Cette interprétation se renforce encore par le renvoi exprès du texte de l'article 8 à l'article 5: l'autorisation ne concerne que les organismes et personnes visés par l'article 5, qui organise l'accès aux informations du Registre national.

Il découle de cette lecture que ces dispositions ne s'appliquent pas à l'utilisation du numéro de Registre collecté via l'eID, sur la base du consentement exprès du porteur de la carte, en vue de vérifier ou de s'assurer de son identité dans le cadre d'une finalité de traitement commerciale ou publicitaire. On est, en effet, en dehors du système d'information du Registre national puisque, par hypothèse, l'entreprise ne demande ni un accès au Registre en vue de la vérification éventuelle des mentions qui figurent sur la carte, ni ne brigue une utilisation de ce numéro qui serait légitimée par des tâches d'intérêt général confiées par la loi.

Il s'agit, en réalité, d'un traitement directement mis en oeuvre entre deux personnes privées, la personne concernée utilisant volontairement l'eID qui lui a été attribuée, en vue de permettre à son partenaire de contrôler son identité et de s'assurer du lien entre la personne et les autres informations traitées. La collecte d'information se fait d'ailleurs sur une base de légitimité spécifique – le consentement libre et éclairé de la personne concernée – en dehors du caractère obligatoire du traitement dont pourront normalement se prévaloir les responsables du traitement du secteur public, utilisateurs du numéro de Registre national.

On observera enfin que dans ce cadre limité, les deux risques majeurs liés à l'accès au Registre national en tant que base de données (la personne concernée ignore l'accès, et cet accès peut donner lieu à des traitements de masse), disparaissent: la personne concernée est avertie et y consent, et le traitement ne concerne qu'une et une seule personne à la fois.

(42) Cette disposition précitée – cf. note 29 – ne vise que des objectifs bénéfiques pour les administrations et le secteur public.

(43) Les travaux parlementaires étaient très clairs à ce propos: 'Cette finalité du Registre national reste entièrement d'application et est par conséquent définie de manière formelle dans la loi. Dans son avis, la Commission note que le projet assigne au Registre national une fonction supplémentaire, à savoir une fonction d'identification des citoyens. Cette fonction demeure toutefois, comme par le passé, du ressort de la commune à laquelle il appartient, dans le cadre de ses compétences de tenue des Registres de la population et de délivrance des cartes d'identité, de contrôler l'identité des personnes. Les données peuvent toutefois être vérifiées au Registre national, mais il n'est pas vraiment conféré de fonction d'identification au Registre national' (Projet de loi modifiant la loi du 8 août 1983, Exposé des motifs, Doc. Parl., Ch., sess. ord. 2002-2003, n° 2226/01, pp. 7 et 8).

15. Le consentement de la personne versus l'autorisation préalable de l'autorité. Traitement du numéro de Registre national par une entreprise privée. Un conflit entre deux normes a priori égales en cas de traitement du numéro de Registre national par une entreprise privée.

La loi du 8 décembre 1992, en son article 5, énonce qu'un traitement peut être effectué sur la base du consentement préalable de la personne. La loi du 8 août 1983, interprétée strictement, impose une autorisation du comité sectoriel afin de poursuivre un tel traitement (44).

Le conflit de norme rebondit alors à un second niveau de hiérarchie des normes.

L'article 5 de la loi du 8 décembre 1992 est une disposition légale prise en application de la Directive 95/46/CE du 24 octobre 1995. Cette Directive, en son article 7, prévoit, en effet, les conditions qui prévalent à la poursuite d'un traitement de données à caractère personnel. Le consentement 'indubitable' est indiqué comme premier fondement de la légitimité du traitement. Il convient tout de suite de souligner que l'autorisation préalable d'une autorité publique n'est, par contre, pas reprise dans la liste des fondements de légitimité des traitements prévue à l'article 7 de la Directive. Du reste, aucune disposition de la Directive ne permet à l'Etat membre de limiter les droits et obligations qui découlent de cette disposition.

Il faut ensuite relever que l'article 20 de la Directive prévoit la possibilité pour l'autorité de contrôle nationale de procéder, dans le cadre des procédures de notification ou déclarations préalables, à un véritable contrôle préalable 'des traitements qui présentent des risques particuliers au regard des droits et libertés des personnes concernées'. Les considérants 53 et 54 donnent une interprétation large de la disposition. Le premier invite les Etats membres à prendre en considération la nature, la portée ou les finalités desdits traitements, telles que celles d'exclusion des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat, ou du fait de l'usage particulier d'une technologie nouvelle. Ils relèvent aussi que l'intervention peut prendre la forme d'un avis ou d'une autorisation de données, en fonction du droit national. Le législateur belge n'a pas mis formellement en oeuvre cette disposition, dès lors que l'autorisation du comité sectoriel est indépendante de la procédure de déclaration devant la Commission de la protection de la vie privée. Il n'empêche qu'il pourrait s'en prévaloir a posteriori pour se justifier.

Enfin, et surtout, l'article 8 de la Directive, qui embrasse les catégories particulières de traitements, indique que les Etats membres déterminent les conditions dans lesquelles 'un numéro national d'identification ou tout autre identifiant de portée générale peut faire l'objet d'un traitement'.

Reste à savoir comment concilier ces deux dernières dispositions avec l'article 7 précité. Un Etat peut-il par le biais d'une disposition relative aux compétences et pouvoir de l'autorité de contrôle modifier les règles de fond de protection relatives aux conditions de légitimation des traitements? La compétence qui lui est laissée de régler les conditions du traitement d'un numéro d'identification national, va-t-elle

(44) Il convient de rappeler qu'une fois les conditions spécifiques d'accès arrêtées par la loi sur le Registre national, le comité ne fera que vérifier si le prescrit et la protection de la loi du 8 décembre 1992 sont bien respectés dans le cadre du traitement projeté.

jusqu'à lui permettre de s'immiscer dans le traitement issu de la collecte directe du numéro auprès de la personne et avec son consentement?

16. L'autorisation préalable du comité sectoriel contraire au principe d'harmonisation complète? Rappel des principes d'interprétation de l'arrêt ASNEF. Le conflit entre l'article 7 et les articles 8 et 20 de la Directive doit s'éclaircir de la jurisprudence de la Cour européenne de justice qui dans un cas analogue (45), a arrêté des principes d'interprétation assez clairs de la Directive en général et de son article 7 en particulier.

En l'espèce, la loi espagnole sur la protection des données prévoyait des règles particulières de légitimation des traitements. Elle considérait notamment que le traitement et la cession de données à caractère personnel étaient possibles sur la base du consentement ou, à défaut, *mais pour les seules données figurant dans des sources accessibles au public*, au sens de la réglementation espagnole, sur la base de la pondération d'intérêt transposant celle de l'article 7, f) de la Directive (46).

Deux associations professionnelles – l'une du secteur du crédit, l'autre du secteur du marketing direct – saisissent une juridiction espagnole considérant que le droit espagnol ajoute une condition à la cause de légitimation inscrite à l'article 7, f) de la Directive 95/46, à savoir que les données en cause doivent figurer dans des sources accessibles au public pour bénéficier d'une pondération d'intérêt favorable, comme fondement du traitement.

La juridiction saisit alors la Cour européenne de justice de deux questions préjudicielles. La première est de savoir si l'article 7, f) de la Directive s'oppose à une réglementation nationale qui, en l'absence de consentement de la personne, et pour autoriser le traitement de données nécessaires à la réalisation d'un intérêt légitime du responsable ou des tiers auxquels les données sont communiquées, exige que les données figurent dans des sources accessibles au public. La seconde interroge la Cour s'il convient d'attribuer un effet direct à l'article 7, f).

La Cour rappelle d'abord que l'harmonisation des législations nationales par la Directive est en principe complète (§ 29). C'est au regard de cet objectif qu'il faut comprendre que l'article 7 de la Directive prévoit une liste exhaustive et limitative des cas dans lesquels un traitement peut être considéré comme étant licite (§ 30). Il s'ensuit, selon la Cour, que les Etats Membres ne sauraient ajouter de nouveaux principes relatifs à la légitimation des traitements à ceux inscrits dans l'article 7 de la Directive, ni d'ailleurs prévoir des exigences supplémentaires qui viendraient modifier la portée de l'un des six principes prévus à cette disposition (§ 31).

La Cour souligne que si l'article 5 de la Directive prévoit de manière générale que '*Les Etats membres précisent, dans les limites des dispositions du présent chapitre,*

(45) Arrêt du 24 novembre 2011, ASNEF et FECEMD, C-468/10 et C-469/10, disponible sur le site www.curia.europa.eu.

(46) L'article 7, f) de la Directive 95/46/CE énonce que: '*Les Etats membres prévoient que le traitement de données à caractère personnel ne peut être effectué que si: (?) f) il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1^{er} paragraphe 1^{er}.*'

les conditions dans lesquelles les traitements de données à caractère personnel sont licites', cette disposition ne remet pas en cause la règle qui précède: les Etats membres ne peuvent agir que dans les limites du chapitre II de la Directive et donc, celles imposées par son article 7. Autrement dit encore, si les Etats membres peuvent préciser les principes inscrits à l'article 7, ils ne peuvent prévoir des exigences supplémentaires qui en modifient la portée, voire d'autres principes que ceux repris par la disposition (§ 35 et 36).

Suite à une analyse précise de l'article 7, f) et de la portée de la pondération d'intérêts qu'elle implique, la Cour considère en réponse à la première question préjudicielle qu'en l'espèce, la législation espagnole est contraire à l'article 7, f), puisqu'elle empêche que certaines catégories de données – celles non accessibles au public – puissent être traitées sur la base de la pondération d'intérêts inscrite à l'article 7, f) de la Directive (§ 49).

La Cour rappelle ensuite que selon sa jurisprudence constante, les particuliers sont fondés à invoquer devant leurs juridictions nationales et à l'encontre de l'Etat, les dispositions d'une Directive qui apparaissent, du point de vue de leur contenu, inconditionnelles et suffisamment précises (§ 51). Tel est le cas de l'article 7, f) de la Directive auquel la Cour reconnaît alors un effet direct (§ 52 et 55).

17. L'autorisation préalable du comité sectoriel contraire au principe d'harmonisation complète? Application des principes d'interprétation de l'arrêt ASNEF. Tout comme dans l'affaire soumise à la Cour, se pose en l'espèce la question de savoir si l'interprétation stricte des articles 5 et 8 de la loi du 8 août 1983 imposant pour toute utilisation et tout traitement du numéro de Registre national une autorisation préalable du comité sectoriel n'a pas pour conséquence d'ajouter une condition de licéité à celles prévues de manière limitative par l'article 7 de la Directive. Si le responsable du traitement peut fonder l'utilisation du numéro de Registre national par le consentement libre et éclairé de la personne concernée, visé à l'article 7, a) de la Directive, l'Etat belge peut-il soumettre la licéité de ce traitement à une condition supplémentaire, l'autorisation du comité sectoriel?

Le principe énoncé par la Cour est clair et ne souffre aucune difficulté d'interprétation: l'Etat membre ne peut ajouter une condition à la liste de l'article 7, qui ne retient pas l'autorisation préalable d'une autorité de contrôle comme source de licéité d'un traitement.

Il faut néanmoins tenir compte des deux autres dispositions précitées.

L'article 8 de la Directive vise des catégories particulières de traitements. Il s'agit principalement des données sensibles qui sont interdites de traitement, sauf dans certaines circonstances prévues par cette disposition. Il convient de remarquer que l'autorisation préalable n'est pas non plus visée dans les exceptions prévues pour lever l'interdiction de traitement des données sensibles.

En son § 7, l'article 8 charge les Etats membres de déterminer les conditions dans lesquelles un numéro national d'identification peut faire l'objet d'un traitement. Cela suffit-il pour permettre à l'Etat membre d'ajouter une condition de licéité non prévue par l'article 7? Nous pensons que non. Il nous semble, en effet, qu'il faut ici tenir un raisonnement analogue à celui tenu par la Cour dans l'arrêt précité. En dehors de l'article 13 qui ne prévoit, du reste, pas de dérogation possible à l'article 7,

les Etats membres n'ont d'autres marges de manoeuvre que de préciser les cas de licéité prévus à cet article. Il est interdit, souligne la Cour, à un Etat membre de prendre une mesure nationale qui prévoit des exigences supplémentaires modifiant la portée d'un principe visé à l'article 7 de la Directive (§ 35). La Cour l'a confirmé expressément au regard de l'article 5 de la Directive, qui indique de manière générale que les Etats membres doivent préciser les conditions de licéité de traitement. Une telle précision n'emporte pas le pouvoir de modifier le régime de l'article 7.

Le § 7 de l'article 8 ne prévoit, lui non plus, aucune dérogation expresse permise aux Etats membres concernant les conditions de l'article 7. Il ne parle certes pas de 'précision', mais de 'détermination' des conditions de licéité du traitement. Nous ne pensons cependant pas que cela suffise à permettre à un Etat de 'déterminer' des conditions qui modifieraient la portée des exigences de l'article 7.

Quant à l'article 20 de la Directive qui permet aux autorités de contrôle nationales d'effectuer un contrôle préalable des traitements susceptibles de présenter des risques particuliers, il ne prévoit pas non plus que, ce faisant, les Etats membres pourraient modifier la portée et le contenu de l'article 7 de la Directive. Certes, le considérant 54 n'exclut pas que le contrôle préalable prenne la forme d'une autorisation préalable, mais il va de soi qu'il faut tenir compte, 20 ans plus tard, des acquis de l'implémentation de ce texte et de leur interprétation par la Cour. Or, une autorisation préalable constitue nécessairement une condition de licéité supplémentaire à l'article 7 de la Directive. Il nous paraît a priori conforme à l'interprétation actuelle de la Cour et à l'importance essentielle reconnue au principe d'harmonisation complète de considérer qu'un Etat membre ne pourrait contourner la jurisprudence précitée et l'interdiction qui en découle par le biais de l'octroi de compétences spécifiques d'autorisation reconnues à l'autorité de contrôle.

En outre, on peut également se demander si l'étendue donnée à l'autorisation, qui revient à une interdiction pure et simple d'utilisation du numéro de Registre national pour toute finalité purement commerciale (47), peut se justifier par une quelconque dangerosité du traitement en cause, au vu de l'analyse des risques faites précédemment. Comme le rappelait le considérant 54 lui-même, les risques visés sont, par essence, très restreints dans le cadre global des traitements tels que protégés par les autres principes protecteurs de la Directive.

Cette disposition n'a, du reste, pas été utilisée par le législateur belge comme permettant à la Commission de la protection de la vie privée d'autoriser certains traitements en modifiant le système de déclarations préalables prévu par la loi du 8 décembre 1992. Le législateur de 2003, quand il modifie la loi sur le Registre national et institue le principe de l'autorisation préalable du comité sectoriel, se réfère seulement à l'article 8 précité de la Directive.

(47) On peut également se poser des questions sur la conformité du système avec l'article 4 de la Directive 2000/31/CE du 8 juin 2000 relative à certains aspects juridiques des services de l'information et notamment du commerce électronique, dans le marché intérieur ('Directive sur le commerce électronique') qui, rappelons-le, prévoit le principe de non-autorisation préalable impliquant notamment que l'exercice de l'activité d'un prestataire de la société de l'information ne soit pas soumis à une autorisation préalable. Or, l'utilisation de l'outil d'identification que représente le numéro de Registre national est, le cas échéant, inhérent à une telle activité, si on considère qu'un tel numéro permet seul une identification quasi certaine dans le cadre de l'octroi du service.

Nous concluons de cette analyse que l'on peut raisonnablement considérer que le régime belge actuel relatif au traitement et à l'utilisation du numéro de Registre national est sérieusement critiquable au regard de la Directive 95/48.

18. Vers une nouvelle question préjudicielle à la Cour de justice de l'Union européenne? Dans ces circonstances, il nous paraît probable qu'une juridiction belge soit amenée à se prononcer sur le conflit exposé ci-avant et que la Cour de Justice soit alors interrogée sur la contrariété potentielle du régime belge d'utilisation du numéro de Registre national, tel qu'existant aujourd'hui, avec la Directive 95/48 en général, et son article 7 en particulier.

Un conflit de norme pourrait bien surgir à un troisième niveau.

On peut, en effet, se demander si l'Etat belge ne pourrait pas se fonder sur l'article 8 de la C.E.D.H. et l'article 22 de la Constitution qui légitime et fondent les législations protectrices de la vie privée et, partant, les mesures nationales de sauvegarde de celles-ci. Or, tel est bien l'objet du régime d'autorisation préalable du comité sectoriel. Cette approche remet alors en cause la validité même de l'interprétation de la Directive par la Cour de justice.

On rappellera simplement ici que les juridictions nationales n'ont pas a priori le droit de statuer sur la validité d'un acte communautaire, ce qui relève de la compétence de la Cour européenne et qu'en vertu du principe de la primauté du droit de l'Union, l'invocation de dispositions de l'ordre national – fussent-elles d'ordre constitutionnel – ne saurait affecter l'effet du droit de l'Union sur le territoire de cet Etat (48). L'article 7, f) de la Directive s'imposerait donc a priori à tout juge national belge qui serait saisi d'une contestation relative à la validité du système d'autorisation préalable du comité sectoriel, pour toute utilisation du numéro de Registre national.

Dès lors, à défaut de pouvoir prévoir avec certitude la réponse qu'apporterait la Cour à la question préjudicielle qui lui serait posée, gageons que le droit européen pourrait bien relancer le débat autour de l'utilisation de ce numéro dans le cadre de l'e-commerce.

19. Conclusions. La problématique de l'utilisation de l'eID dans le cadre de l'e-commerce est pour le moins paradoxale.

D'une part, son utilisation est clairement prônée par les autorités, qui vantent sans cesse les vertus tant de ses fonctions de signature que de la sécurité juridique qu'elle implique concernant l'identification du porteur. D'autre part, son utilisation est – comme l'a souligné la Cour des comptes dans son rapport précité – freinée par l'insécurité juridique qui règne autour de l'utilisation du numéro de Registre national, laissé en accès libre sur l'eID.

La condition de l'obtention d'une autorisation préalable du comité sectoriel du Registre national pour tout traitement du numéro de Registre national revient, en réalité, à interdire cette utilisation par le secteur privé, hors exception légale, principalement la nécessité de cette utilisation pour une tâche d'intérêt général. L'arrêt de la

(48) Arrêt du 26 février 2013, Melloni et Fiscal, C-399/11, § 59, disponible sur le site www.curia.europa.eu.

Cour d'appel de Bruxelles du 9 mai 2012, commenté ci-avant, confirme cette constatation.

La présente étude a montré que l'on peut sérieusement s'interroger sur l'opportunité et la légalité de l'application du système d'autorisation préalable par le comité sectoriel à un traitement du numéro de Registre national par le secteur privé, sans accès au Registre national, sur la base du consentement libre et éclairé du porteur de l'eID et dans le respect de la loi du 8 décembre 1992.

Outre que l'on ne comprend pas bien en quoi une telle utilisation présenterait des risques tels pour les libertés individuelles qu'une procédure – exceptionnelle – d'autorisation préalable soit prévue, la nécessité de recourir dans cette hypothèse à l'autorisation préalable du comité sectoriel est apparue critiquable au vu du texte même de la loi du 8 août 1983 et d'une lecture combinée de ses articles 1^{er}, 5 et 8.

Au surplus, et pour autant que l'on admette que cette autorisation s'impose, naît un conflit entre deux conditions de licéité du traitement du numéro de Registre national: le consentement libre et éclairé de la personne, qui suffit en règle générale à légitimer les traitements de données à finalité commerciale et de marketing direct, et l'autorisation préalable du comité sectoriel.

Il nous est apparu ensuite, sur la base de la jurisprudence de la Cour de justice de l'Union européenne, que l'exigence supplémentaire d'une autorisation préalable à celle du consentement de la personne paraissait également critiquable au regard de l'interprétation donnée à l'article 7 de la Directive 95/46, dont les principes de protection des données sont contenus dans la loi du 8 décembre 1992.

Reste à savoir ce que nous réservera l'avenir.

Lors de notre réflexion, nous avons souligné notre compréhension quant à l'application d'un système d'autorisation préalable dans le cadre d'une demande d'accès au Registre national et du système de communication d'informations qu'il met en oeuvre, conformément aux finalités légales qui lui sont explicitement attribuées, sous réserve de sa conformité au droit européen.

Sous peine de voir le système entier condamné par la Cour de justice, ne vaudrait-il pas mieux adopter une lecture raisonnable des dispositions de la loi du 8 août 1983?

PortiSign™: Système de dématérialisation des contrats d'assurances

Claude Rapoport (1)

(1) © Portima 2012. Tous les droits de propriété intellectuelle relatifs au système PortiSign tel que décrit dans le présent article appartiennent à Portima SCRL.