BRUSSELS PRIVACY HUB
WORKING PAPER
VOL. 5 • N° 15 • JANUARY 2019

BRUSSELS PRIVACY HUB
Vrije Universiteit Brussel

BELGIUM, COURTS, PRIVACY AND DATA PROTECTION. AN INVENTORY OF BELGIAN CASE LAW FROM THE PRE-GDPR REGIME (1995-2015)

by Paul De Hert[1]

This Contribution focuses on the use made by the Belgian Constitutional Court, the Cour de Cassation and the ordinary courts of the right to privacy and the right to have personal data protected as anchored in the Belgian Constitution, the Belgian Data Protection Act and the European sources. A selection of their judgements, all dating from the era before the new EU Data Protection Regulation, are discussed along the lines of their impact on health privacy, workplace privacy, surveillance and social media privacy. Our analysis shows a great deal of European loyalty on behalf of the Belgian Constitutional Court towards European trends to favour privacy and data protection. In stark contrast stands the case law of the Cour de Cassation mainly focussed at preserving prosecutorial interests and employer's interests at the detriment of privacy and data protection interests. In our conclusions we discuss tendencies towards cosmopolitanism and tribalism, the dramatic impact of evidence law and patterns of litigation.

Our analysis covers the data protection era where Belgian law was indirectly governed by EU Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23 November 1995, 31). The Directive contributed to the roll-out of data protection and harmonized the data protection provision in the EU Member States but suffered from implementation weaknesses and lack of recognition. A certain lack of recognition of the importance of data protection in the European (and Belgian legal) landscape disappeared with the the EU General Data Protection Regulation 2016/679 ("GDPR") (OJ L 119, 5 Ma.2016, 1–88) that repealed Directive 95/46/EC and came into force on 25 May 2018 with direct applicable provisions. Further studies are needed to study the impact of the new European provisions on the work and output of the Belgian courts.

Keywords: Belgian Constitutional Court, Belgian Cour de Cassation, Belgian ordinary courts, Belgian and European provisions on the right to privacy and the right to have personal data, constitutional patriotism, exit strategy, evidence law

Contents

The Brussels Privacy Hub Working Papers are intended to circulate research in progress for comment and discussion. Available at www.brusselsprivacyhub.org/publications.html
ISSN N° 2565-9979. This version is for academic use only.
Parts of this paper have been used in P. De Hert, 'Courts, 'Privacy and Data protection in Belgium: Fundamental rights that might as well be struck from the Constitution', in Maja Brkan & Evangelia Psychogiopoulou (Eds.), Courts, Privacy and Data Protection in the Digital Environment, Cheltenham: Edward Elgar Publishing Ltd, 2017, 63-81.

Disclaimer

1. Introduction

1.1. The Constitutional Framework (Article 22 Belgian Constitution)

The original 1831 Belgian Constitution (the Constitution) included two privacy-related provisions: Article 22 on the confidentially or secrecy of postal letters (now Article 29) and Article 10 on the inviolability of the home (now Article 15).

Like other countries it was only in the twentieth century that a general privacy right was included. The 'right to respect for his or her private life' solely became a fundamental right in 1994 thanks to the incorporation of Article 22 in the revised 1994 Constitution[2]: ***"Everyone is entitled to respect of his private life and his family life, except in the cases and under the conditions determined by law. The law, the decree or the in Article 134 stipulated ruling guarantee the protection of that right".***[3]

In the ***parliamentary discussions*** it was stated that: *"**Article 22 should have the same meaning and interpretation as Article 8 ECHR (the 1950 European Convention of Human Rights)**"*. [4] This intention to align the protection provided by Article 22 Constitution and the one offered by Article 8 ECHR has been confirmed in several judgments of the Belgian Constitutional Court. For instance, on 10 November 2011 the Court stated that: "***it appears from the preparatory work that the legislator sought to put as much as possible of Article 22 in accordance with Article 8 ECHR in order to avoid disputes on the respective contents of Article 22 Constitution and Article 8 ECHR***"[5]. As a consequence, case law and legal authors, following in the footsteps of the European Court on Human Rights (the ECtHR), have given a broad application to Article 22 Constitution[6] similar to the one given to Article 8 ECHR.

Besides establishing affiliation with Article 8 ECHR, the parliamentary discussions emphasised that the new provision also aims at providing protection to the person against "***intrusion, including as a result of the continuous development of information technologies, when measures of search, investigation and control by the government and by private institutions are taken when exercising their functions or activities***"[7]. Hence, although Article 22 Constitution does not expressly refer to the use of new technologies or to the idea that personal data must be protected

1 Full professor Vrije Universiteit Brussel; associated professor Tilburg University. The author is grateful to Yung Shin Van Der Sype, Laura Jacques, Ronny Saelens and Amy Weatherburn.
2 See for the full text, http://www.const-court.be/en/basic_text/belgian_constitution.pdf.
3 The other provisions mentioned above remained unaltered but where shifted within the Constitution. The principle of the inviolability of the private home is now contained in Article 15 Constitution. Article 29 Constitution provides for the right to the secrecy of letters. All other forms of private communication fall under the scope of the general protection of privacy, guaranteed by the new (content-wise) Article 22 Constitution and Article 8 ECHR. For more in detail, see Marie-Aude Beernaert & Philip Traest, 'Belgium: From Categorical Nullities to a JudiciallyCreated Balancing Test' in Stephen C. Thaman (ed.), ***Exclusionary Rules in Comparative Law*** (Springer 2013) (161-183) 172-174.
4 Chamber, Parliamentary Documents, 1992-93, 997/5, 2. See http://www.dekamer.be/digidoc/DPS/K2342/K23422521/K23422521.pdf.
5 CC, No. 176/2011, 10 November 2011.
6 Paul De Hert, *Artikel 8 EVRM en het Belgisch recht. De bescherming van privacy, gezin, woonst en communicatie* (Mys & Breesch 1998).
7 Senate, Parliamentary Documents, 1991-92, 100-4/5, 3.

when processed through new technologies, it is clear that the drafters had the intent to incorporate personal data protection concerns into the newly created provision.[8]

Furthermore, Article 22 Constitution imposes the obligation that derogations to the right to private life must be enshrined in formal law. To this, the Council of State (CS) has added the requirement to pay respect to at least the 'minimal standards' outlined in the Belgian (Federal) Data Protection Act, 8 December 1992.[9]

Note that the requirement in Article 22 Constitution that derogations require a basis in formal law is more protective than what has been spelled out by the ECtHR with regard to Article 8 ECHR where the requirement of a legal basis to make privacy derogations possible does not necessarily require formal law.[10]

1.2. The Belgian Data Protection Legal Framework – The 1992 Data Protection Act

We saw ***above*** that the right to the protection of personal data is not explicitly mentioned in the Constitution. However, like Article 8 ECHR, the right to a private life in Article 22 Constitution is broadly understood to cover all privacy interests including the right to protection of personal information.[11] Contrary to certain other national constitutions and to the EU Charter on Fundamental Rights, there is no separate recognition of a right to protection of personal data next to the right of privacy, at least in the text.

At the level of ordinary legislation, there is a multitude of laws protecting the rights to privacy, secrecy of letters and the inviolability of the private home.[12] This framework has been complemented in the past decades with several data protection acts and provisions. The central legislative tool in Belgium was the (federal) Act of 8 December 1992 on the protection of privacy in relation to the processing of personal data (hereafter, the 1992 Data Protection Act).[13] This general data protection act implements the Directive 95/46/EC and is applicable to any operation or set of

8 Els Kindt, Eva Lievens, Eleni Kosta, Thomas Leys & Paul De Hert, 'Constitutional Rights and New Technologies in Belgium' in Ronald Leenes, Bert-Jaap. Koops & Paul De Hert (eds.), *Constitutional Rights and New Technologies. A Comparative Study* (T.M.C. Asser Press 2008) 11-56.

9 See the discussion of the Council of State in CC, No. 202/2004, 21 December 2004, para B.5.4 and B.20: " Finally, the requesting parties inquire what the treatment will be of the the data thus collected. In reply to a question about this from the Council of State, the Government stated that "to the extent that neither the Act of 8 December 1992 on the protection of privacy with regard to the processing of personal data nor the present draft law explicitly provides for exceptions, [...] it goes without saying (...) that the information obtained will be treated in accordance with that law (*Parl. St.*, Kamer, 2001-2002, DOC 50-1688/001, p. 111). With the application of that Act, the right to the protection of privacy is therefore guaranteed."

10 For instance, the CC, No. 202/2004, 21 December 2004, para B.5.4.: "Although Article 8.2 of the aforementioned European Convention, uses the term "law" this does not require a "law" in the formal sense of the word. The same term "law", used in Article 22 Constitution, requires a statutory provision. This constitutional requirement is imposed on the Belgian legislator, under Article 53 of the European Convention that provides that nothing in the Convention shall be construed as limiting or derogating from any of the human rights and fundamental freedoms which may be ensured under the laws of any High Contracting. See Paul De Hert, 'Artikel 8 EVRM. Recht op privacy' [Article 8 of the Convention on Human Rights. The Right to Privacy] in Johan Vande Lanotte & Yves Haeck (eds.) ***Handboek EVRM. Deel 2 Artikelsgewijze Commentaar*** (Intersentia, 2004) 705-788. See in identical terms, CC, No. 29/2010, 18 March 2010, B.10.2

11 Antonella Galetta & Paul De Hert, 'Mapping the legal and administrative frameworks in Belgium' in *Increasing Resilience In Surveillance Societies, Deliverable D5: Exercising Democratic Rights Under Surveillance Regimes* (2014), http://irissproject.eu/wp-content/uploads/2014/06/Belgium-Composite-Reports-Final1.pdf

12 A selective overview (related to criminal law) is given by Marie-Aude Beernaert & Philip Traest, 'Belgium', ***supra,***172-180.

13 Official Journal 18 March 1993.

operations performed on personal data by private and public entities.[14] It sets up a list of principles and obligations very similar to the provisions of the EU Directive. Note that the Act contains many criminal sanctions many linked to the neglect of practically all data protection duties. The central actor in the Act is the Belgian Data Protection Authority, commonly called 'the Privacy Commission' of 'Commission for the Protection of Privacy'.[15] Note that this authority has no administrative sanctioning powers. It acts as a mediator or Ombudsman in disputes, although it can, when necessary, turn to the criminal law system (prosecutor, investigative judge) in the hope that they instigate criminal proceedings.

Early 2018 saw the publication of the Act of 3 December 2017 creating the Data Protection Authority (Official Journal, 10 January 2018, 989-1008), an Act that replaces the Commission for the Protection of Privacy) by a new authority with more extensive powers, including the power to impose administrative sanctions, and gives full effect to the GDPR provisions in this regard.

The 1992 Data Protection Act has been complemented by a variety of sectorial laws such as the CCTV Act of 2007[16] which imposes additional obligations on the data collector that uses a video-surveillance camera (restricted to the law enforcement sector) or the Collective Labour Agreement No. 81 regulating the rights to privacy and data protection in the workplace and Collective Labour Agreement No. 68 regulating the rights to privacy and data protection with regard to CCTV at the workspace. [17]

Note that on 5 September 2018, the new Belgian Act of 30 July 2018 (the 2018 Data Protection Act) was published in the Belgian Official Journal (Official Journal, 5 September 2018, 68616-68684), replacing the 1992 Data Protection Act and complementing the direct applicable GDPR provisions with complementary and clarifying provisions.

1.3. The Highest Jurisdictions in Belgium

The Belgian court structure is very similar to its neighbouring countries (the Netherlands and France): a hierarchical system of administrative courts and ordinary courts. The ordinary court system is composed of 187 Justices of Peace, 32 Police Courts, 27 Courts of First Instance, 27 Labour Courts and 27 Commercial Courts, 5 Courts of Appeal and at the top a Supreme Court, the highest civil and criminal court, composed of three chambers (civil and commercial matters; criminal matters and labour matters).[18] Case law precedents have no legally binding force, but the decisions of the highest courts have strong persuasive authority, especially when they are confirmed repeatedly.[19] A relatively newcomer to this judicial structure is the Constitutional Court as it was created on 2 October 1984.

This Constitutional Court (***Court Constitutionelle, Grondwettelijk hof***) is the guarantor of the

14 The Privacy Commission, 'Protection of personal data in Belgium' <http://www.privacycommission.be/sites/privacycommission/files/documents/protection-of-personal-data-inbelgium.pdf> accessed 8 April 2015.
15 *Commissie voor de bescherming van de persoonlijke levenssfeer/Commission de la protection de la vie privée.*
16 CCTV Act (2007) Official Journal. 21 March 2007.
17 Collective Labour Convention No.81 (2002) Official Journal, 29 June 2002 and Collective Labour Convention No. 68 (1998) Official Journal 2 October 1998
18 Baker & McKenzie, ***Dispute Resolution Around the World. Belgium***, (2013) 3-6 at http://www.bakermckenzie.com/files/Uploads/Documents/Global%20Dispute%20Resolution/Dispute%20Resolution%20Around%20the%20World/dratw_belgium_2013.pdf.
19 Baker & McKenzie, ***Dispute Resolution Around the World. Belgium***, (2013) ***supra*** note 18, 1.

fundamental rights enshrined in the Constitution. Its history is linked to the transformation of Belgium from a unitary state into a federal state, with different legislative assemblies. Hence the creation in 1984 of a Court of Arbitration, serving from 1985 on as an arbiter in conflicts of jurisdiction between the different entities. In the years to follow the Court evolved into a full-blown constitutional court with enlarged review powers and a new name (the Constitutional Court'). This Constitutional Court is competent to review the legislative acts adopted by the federal parliament (statutes) and by the parliaments of the communities and regions (decrees and ordinances) and to amend partially or annul the entire act reviewed which is found to be in violation with the Constitution.[20] A case can be brought before the Court by any authority designated by statute, any person who has a justifiable interest, or, in a 'preliminary procedure', any court of law.[21] Over these last years, several acts have been subject to review by the Constitutional Court regarding Article 22 Constitution in conjunction with Article 8 ECHR, often in response to questions put to the Court by lower courts ('preliminary procedure').[22]

The rulings of the Court are often met with acceptance, also by authorities. In general, it cannot be said that the Court engages in judicial activism, in the sense that is has developed scrutiny and case law beyond the standards set by the ECtHR or the European Court of Justice. Several reasons account for the rather lenient approach adopted, especially towards the legislator, the Belgian Parliament, who appoints the members of the Constitutional Court, of which half of them are former politicians.[23] Contrary to constitutional courts in for instance Germany and the United Kingdom, one cannot say that the Belgian Court provides for stricter scrutiny than the ECtHR in areas such as privacy and data protection.[24] The Court has equally shown almost no desire to explore the particularities of the Belgian Constitution and to go further or above the standards of the European courts when possible. Illustrative of this, is a 2004 judgment on the constitutionality of certain 'novel' investigation techniques for the criminal law enforcement authorities introduced by a 2003 Act in the Code on Criminal Procedure.[25] One of the proposed powers dealt with the interception and opening of classical mail.[26] The applicants were of the opinion that these provisions violated Article 29 Constitution that contains an absolute protection, unless for letters entrusted to postal services.[27] In a remarkable move, questionable from the perspective of Article 53 of the ECHR, the Constitutional Court invoked the "***non-absolute phrasing of other***

20 Patricia Popelier, 'The role of the Belgian constitutional court in the legislative process' (2005) 26(1) *Statute Law Review*, 22-40.
21 See more in detail on these two different procedures or *modi operandi* https://en.wikipedia.org/wiki/Constitutional_Court_of_Belgium.
22 CC, No. 139/2013, 17 October 2013; CC, No. 108/2006, 28 June 2006; CC, No. 96/2008, 26 June 2008.
23 Patricia Popelier & Catherine Van De Heyning, 'Procedural Rationality: Giving Teeth to the Proportionality Analysis' (2013) 9 European Constitutional Law Review, 230, 245.
24 For a discussion of constitutional courts in Europe that offer a more intensive and comprehensive protection of fundamental rights on the basis of their own constitution or constitutional principles, with, as examples, the respect to the protection of personal mail and communication recognised by the German Constitutional Court and the British House of Lord's case-law on the protection of privileged correspondence between a lawyer and his or her client, see Patricia Popelier & Catherine Van De Heyning, ***supra*** note 25, 230-262, 247-248.
25 The following ***special investigation methods*** were introduced in the CCP: observation, infiltration and the operation of informants (article 47 § 1 of the code of criminal proceedings.). The 2003 Act also introduced ***other methods of*** investigation: interception and opening of classical mail, direct monitoring, postponed intervention, looking-in operations and the collection of data regarding bank accounts and -transactions. These powers are categorised as 'other', because they are considered as more traditional. See on this Act of 6 January 2003 H. Berkmoes & J. Delmulle, ***Les méthodes particulières de recherche et quelques autres méthodes d'enquête***, (Politeia 2008) 718p; C. De Valkeneer, ***Manuel de l'enquête pénale*** (Larcier 2005) 197-245.
26 Articles 46ter and 88sexies of the Code of Criminal Procedure.
27 "The letter is inviolable. The law determines which officials may violate the confidentiality of letters entrusted to the postal service".

constitutional provisions and international treaties" to allow for powers that were violating this absolute right enshrined in Article 29 Constitution.[28]

Apart from the Constitutional Court, the right to privacy is mainly invoked before the ***Cour de Cassation*** (***Hof van Cassatie***).[29] The ***Cour de Cassation*** is the court of highest instance as it only examines the legal validity of judgments delivered by the Courts of Appeal. On this basis, it may only confirm or quash the Appeal Court's decision and refer it to another court.

Like the Constitutional Court, the ***Cour de Cassation*** follows the Article 8 ECHR logic with regard to privacy. Without a great willingness to uphold privacy claims in conflicts, it likes to stress that the right to the protection of one's private life guaranteed by Article 8 ECHR is not absolute and may be subject to restrictions, in this case the ones listed in Article 8(2) of the ECHR: the restriction must be established by law (legality principle); must work towards one of the enumerated goals of Article 8(2) (principle of finality); and must be necessary in a democratic society for the realisation of that goal (principle of proportionality). [30] Not strictly adhering to the text of Article 22 Constitution (***above***), the ***Cour de Cassation*** aligns itself with the jurisprudence of the ECtHR by recognising that, for the purposes of applying Article 8 ECHR, "***the term 'law' means any rule of internal law, written or otherwise, provided that it is accessible to the persons concerned and is stated in a precise manner"***[31].

While the Constitution does not contain any clause relating to the horizontal effect of fundamental rights[32], the ***Cour de Cassation*** held in the 2001 ***Leli's World*** judgment (that will be discussed ***below***) that Article 8 ECHR also applies to conflicts between private parties. There were precedents in the case law of lower courts[33] recognising the horizontal effect of the ECHR, but this was the first time that the horizontal effect of the ECHR was acknowledged by the Supreme Court itself.[34] Interesting in this regard is that the ***Cour de Cassation*** in these 'horizontal cases' makes use of the criteria for privacy derogations found in the second paragraph of Article 8 ECHR (legality, proportionality and legitimacy), although this provision is not really designed to govern horizontal situations.

In general, the ***Cour de Cassation*** is not a forerunner in terms of upholding civil liberties. Changes in case law expanding the reach of civil liberties are most often the result of case law of the

28 CC, 21 December 2004, No. 202/20, para B.12.2. "Although confidentiality, at the moment of the adoption of the Constitution, could be understood in absolute terms, today it needs to be read in the light of other constitutional provisions and international treaties may now, in order to determine its scope. Articles 15 and 22 Constitution, or the inviolability of the home and the right to respect for private and secure family life, are linked to article 29 and assume the same will of the Constituent to protect the individual in his private atmosphere in order to enable its development and deployment. Although Article 29 Constitution provides explicitly no restriction on the fundamental right enshrined in it, such a restriction may be justified, however, if it is necessary to ensure the observance of other fundamental rights. Rights such as the freedom of the person (Article 12, first paragraph, Constitution), the right to life (Article 2 of the European Convention on Human Rights) and the right of ownership (Article 16 Constitution and Article 1 of the First Additional Protocol to the European Convention for the ensuring of Human Rights), oblige the legislator to punish criminal activities infringing these fundamental rights and explain why, allowing restrictions may be necessary to the secrecy of letters provided they are proportionate to the legitimate aim pursued".

29 Judgments of the Court can be found at http:// www.cass.be.

30 An example is *Cour de Cassation*, No. RG P.02.0694.F, 8 January 2003. See Marie-Aude Beernaert & Philip Traest, *supra* note 3, 172.

31 ***Cour de Cassation***, No. RG 8168, 2 May 1990. See Marie-Aude Beernaert & Philip Traest, ***supra*** note 3, 172. However, and more in respect of the Constitution, the ***Cour*** in this judgement refused to consider a guidance note by the executive as a 'law'.

32 Els Kindt, Eva Lievens, Eleni Kosta, Thomas Leys & Paul De Hert, *supra* note 8, 11-56.

33 Paul De Hert, *supra* note 7, 54. *Cour de Cassation*, 27 February 2001, (2001) Computerrecht, 202, annotated by Jos Dumortier.

34 Paul De Hert & Mieke Loncke, 'Camera Surveillance and Workplace Privacy Country report Belgium' in Sjaak Nouwt, Berend R. de Vries & Corien Prins (eds.), ***Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy*** (T.M.C. Asser Press, 2005) 167-209.

ECtHR.[35] This approach explains why the ***Cour de Cassation*** rarely gives a high priority to privacy and data protection. Uniquely composed of professional judges taken from ordinary courts and the office of prosecutors, the Court delivers judgment after judgment favouring the interest of the prosecution (in the criminal law sphere) or of employers (in labour law conflicts). It is fair to say that the Court's doctrine on the use of illegally obtained evidence, discussed ***below***, has particularly contributed to eroding (proponents of this doctrine would say 'better balanced') privacy and data protection standards.[36]

Finally, there is the State Council (***Conseil d'Etat/Raad van State***), the highest administrative court. This Court is an advisory and jurisdictional institution created as an appeal institution for individuals and companies that claim to have been harmed due to irregular administrative acts.[37] The State Council may suspend and cancel those acts and provide protection against arbitrary administrative acts. Although, the State Council has not yet ruled on any digital environment cases yet, the Council has already dealt with some data protection cases in other contexts, more often concerning the individuals' rights to anonymity and access to personal information.[38]

1.4. Evidence law and the impact on the protection of privacy and data protection

When discussing the ***Cour de Cassation***, we wrote that its doctrine on the use of illegally obtained evidence has had a strong impact on privacy and data protection standards. This doctrine goes back to the 2003 '***Antigone***' judgment[39] regarding the admissibility of illegally obtained evidence. A judge is allowed to use illegally obtained evidence when the illegal act is of a minor nature compared to the offence that the first act enabled to demonstrate.[40] As long as the illegal acts do not affect the reliability of the evidence or do not infringe the right to a fair trial, use of illegally obtained evidence in courts is the rule. Before 2003, rules on evidence law were strict and domestic courts systematically rejected the evidence of the employer when it was contrary to legislation related to the right to private life.[41] This changed with the ***Antigone*** case and today more and more evidence obtained through privacy infringing acts by employers and police officials is used in court.[42]

35 A good example is ECtHR, ***Van Rossem v. Belgium***, No. 41872/98, 9 December 2004. See on this case Marie-Aude Beernaert & Philip Traest, ***supra*** note 3, 173.

36 Yung Shin Van Der Sype, 'Het doel(-gebondenheidsbeginsel) voorbij. Het trieste lot van de vereiste van verenigbaar gebruik bij het bewijs van het ontslag om dringende reden', (2015) *JTT* No. 1232, 377-482; Yung Shin Van Der Sype, 'Antigoon gesust: Het privédetectiveverslag als bewijs in (on)rechte', (2015) *Oriëntatie*, No. 8, 212-225.

37 Belgian Privacy Commission, 'Conseil d'Etat/Raad van State' < http://www.anthologieprivacy.be/fr/conseil-detat> accessed on 18 April 2015.

38 State Council, Decision of 10 June 1986; State Council, Decision of 10 December 1993; State Council, Decision of February 1995.

39 ***Cour de Cassation***, No P.03.0762.N, 14 October 2003. See for a discussion Marie-Aude Beernaert & Philip Traest, ***supra*** note 3, 161-183.

40 *Cour de Cassation*, No. P.04.1644.F/1, 2 March 2005; Karen Rosier & Steve Gilson, *La vie privée du travailleur face aux nouvelles technologies de communication et à l'influence des réseaux sociaux - L'employeur est-il l'ami du travailleur sur Facebook?* in Le droit du travail à l'ère du numérique (Anthemis 2011) 61, 107.

41 Examples with regard to the inviolability of the home: ***Cour de Cassation***, March 12, 1923, Pass. 1923, I, 323. See on evidence obtained with a violation of this right ***Cour de Cassation***, May 13, 1986, Arr. Cass. 1985-86, 1230; ***Cour de Cassation***, June 16, 1987, Arr.Cass. 1986-87, 1423; Pass. 1987, I, 1278. See with regard to evidence and insurance: ***Cour de Cassation***, April 18, 1985, Arr.Cass. 1984-85, 1102; JT 1985, 421; Pass. 1995, I, 1008. See with regard to employee privacy and evidence ***Cour de Cassation***, February 27, 2001, Soc.Kron. 2001, 455. On this last judgement Paul De Hert & Serge Gutwirth, 'Cassation and secret cameras: more holes than cheese' (2001) Panopticon, 309-318.

42 *Cour de Cassation*, 27 February 2001, No. P.99.0706.N/1.

The new doctrine obviously decreases the protection of the right to privacy and right of personal data. A violation of privacy (Article 8 ECHR) does not have any impact unless it comes together with a violation of the right to a fair trial (Article 6 ECHR). Violations of these rights only lead to exclusion of evidence if the acts to gather the evidence affect the reliability of the evidence or infringe the right to a fair trial. The new doctrine was a great success in the sense that all courts involved had to apply it (the investigation courts, police courts, correctional courts, courts of assize and courts of appeal) fearing the strict supervision of the ***Cour de Cassation*** on this point. Courts even started applying it in areas not connected to criminal law, such as labour law.[43]

Of course, the ECtHR in ***Khan*** (2000) paved the way to this state of cases where the Court attached no real consequences to a violation of Article 8 ECHR in a criminal procedure. The requirement of the fairness of the criminal procedure, laid down in Article 6 of ECHR, is complied with when the entirety of the criminal procedure is fair. The ECHR accepted that unlawfully obtained evidence should not be excluded on the condition that the defendant has not been deprived of the possibility to contest the authenticity of the unlawfully obtained evidence and to oppose its application.

The ***Khan*** dictum, - a violation of Article 8 ECHR does not automatically result in a violation of Article 6 ECHR-, was very quickly acknowledged by the Belgian Courts. The Ghent Court of Appeal led the way with the judgment of 28 March 2002.[44] In this judgment, the Ghent Court of Appeal concluded that the retrieval and the use of surveillance camera images by the police, gathered by the registered office of the National Bank of Kortrijk in Belgium, produced valid evidence. The use of surveillance camera images of the public road to demonstrate the existence of a crime of which the aforesaid bank was not a victim did not constitute a breach of Article 8 of ECHR (privacy) nor of Article 6 ECHR (fair trial). The Ghent Court of Appeal explicitly referred to ***Khan*** and added a crucial paragraph which states that the Court is unwilling to sacrifice its power to balance evidence within the framework of the law of criminal evidence, in favour of a strict application Data Protection Act.

It therefore does not come as a surprise that the ECtHR validated the ***Antigone*** case law (itself referring to ***Khan***) in ***Lee Davies v. Belgium*** (28 July 2009).[45] The Constitutional Court followed in judgments of 22 December 2010 and 27 July 2011 contributing to the full acceptance of the ***Antigone*** doctrine as a fixed part of Belgian criminal procedure.[46]

This 'prosecution-friendly' approach has been met favourably by the Belgian legislator. Already in 2004, the doctrine was embedded in legislation with regard to elements of evidence coming

43 Fabienne Kéfer, 'La légalité de la preuve confrontée au droit à la vie privée du salarié' in Marc Verdussen & Pierre Joassart (eds), *La vie privée au travail* (Anthemis 2011) 17-58; Fabienne Kefer, 'Antigone et Manon s'invitent en droit social - Quelques propos sur la légalité de la preuve - Cass 10/3/08' (2009) J.L.M.B. 325. Some examples of cases where illegally obtained evidence was accepted: *Cour de Cassation*, 9 June 2004, (2004) Arr.Cass, No. 6-8, 1028; (2004) Pas. No. 5-6, 993 ; *Cour de Cassation* 2 March 2005, (2005) Arr.Cass, No. 3, 506, concl. D. Vandermeersch; (2005) Computerrecht, No. 5, 258, annotated by B. Ooms & P. Van Eecke; *Cour de Cassation* 10 March 2008, (2010) NJW No. 218, 195, annotated by K. Van Kildonck;(2008) Soc.Kron. No. 9, 538. See equally Labour Tribunal Liege, 8 March 2011, (2011) Soc.Kron. No. 8, 404; Labour Tribunal Antwerp 18 October 2011 (2010/AA/595); Labour Tribunal Brussels, 18 October 2013 (AR nr. 2012/AB/652). There is so far one unique example where the appliation of *Antigone* has not led tot he acceptance oft he illegally obatined evidence: Labour Tribunal Brussels, 9 September 2016 (2015/AB/624).

44 Ghent, 28 March 2002, (2002) 3 No. 6 Tijdschrift voor Strafrecht 310-317, annotated by P. de Hert.

45 See for a discussion Marie-Aude Beernaert & Philip Traest, *supra* note 3, 170.

46 CC, No. 158/2010, 13925, 22 December 2010 and CC, No. 139/2011, 27 July 2011

from abroad.[47] In 2013 followed general recognition in domestic recognition and incorporation in the Code of Criminal Procedure.[48] The new Article 32 of the Code of Criminal Procedure sets out the three cases where 'illegally obtained elements of evidence' have to be declared invalid and as a result can no longer be used by the judge in his assessment:

- the penalty of nullity is legally prescribed for violation of the procedural rules, or
- the illegal act that has been committed has affected the reliability of the evidence, or
- use of the evidence violates the right to a fair trial.

2. National jurisprudence in the field of privacy and data protection: the position of the domestic constitutional order

2.1. Electronic exchange of health information & Health Information Systems

Health Information Systems - Constitutional Court, 14 February 2008

In 2008,[49] the Constitutional Court considered a case in which it had to decide had to rule on two issues: one related to substantive questions about privacy and data protection; another one about respective powers to vote laws with an impact on privacy and data protection in a federal state like Belgium.[50] The claim concerned the annulment of several provisions of a Flemish Decree that created a Health Information System. The system was designed to ensure the exchange of information between doctors, hospitals and several administrative authorities. Did this system set up in a Flemish Decree respect the standards provided for by the Federal 1992 Data Protection Act?

The applicants, -the Belgian association of medical professionals (***het Verbond der Belgische Beroepsverenigingen van Geneesheren-specialisten***)-, believed this was not the case and argued that the requirements contained in Article 8 ECHR and the 1992 Data Protection Act were not met. Second, they contended that there was a violation of Article 5 of the Special Law of 8 August 1980 on the institutional reforms containing the guidelines for delimitating federal and regional regulatory competences.

In the 2008 judgment the Constitutional Court reminded the regional legislator that he/she is required to take into account the data protection standards enshrined in the Federal 1992 Data Protection Act in its legislative work. Being noncompliant with the 1992 Data Protection Act, the Court's decision cancelled several provisions figuring in the Flemish Decree that created a Health Information System as being in conflict with the federal 1992 Data Protection Act. The Court also

47 Article 13 of the Act of 9 December 2004 concerning international mutual legal cooperation in criminal matters and amending article 90ter of the Code of Criminal Procedure, Official Journal, 24 December 2004.

48 Act of 24 October 2013 amending the Introductory Title of the Code of Criminal Procedure concerning nullity, Official Journal, 11 November 2013. See Jonathan Raeymakers & Benjamin Gillard, 'Legal Embedment of the Antigoon Case Law' (2003) http://www.eubelius.be/en/spotlight/legal-embedment-antigoon-case-law accessed 1 July 2015; Bart De Smet, 'Antigoon-criteria eindelijk wettelijk verankerd, (2013) Rechtskundig Weekblad No. 14, 762.

49 CC, No. 15/2008, 14 February 2008.

50 CC, No. 29/2010, 18 March 2010.

emphasised that the exchange of communication related to health information of an individual constitutes an interference with the right to the private life of patients covered by Article 8 ECHR and Article 22 Constitution. In order to justify such interference, the decree legislator must meet the requirements of legality, proportionality and legitimacy with the aim pursued. The Court further explained that although the regional legislator might organise processing activities in the framework of its competence, he must respect the minimum standards covered by the federal 1992 Data Protection Act[51]. In that respect, the Court verified the compliance of the Decree with the 1992 Data Protection Act and found several flaws in the Decree: a lack of respect of the rule of written consent (Article 7§2 Act),[52] a lack of respect of the rule according to which personal data must only be processed for specific and legitimate finalities and a lack of respect of the proportionality and data minimisation principles (Article 4§3 Act).[53]

Health Information Systems - Constitutional Court, 18 March 2010

The Constitutional Court also had to judge in 2010 on the compatibility of the (Federal) Act of the 21 August 2008 aiming to create an eHealth Platform with the rights to privacy and data protection.[54] This eHealth platform was designed ***not*** to record substantive data centrally, but ***only*** to allow a secure electronic exchange of health information between healthcare professionals (doctors, hospitals, and so on).

The claimants nevertheless asked for an annulment of the Act and argued that the eHealth Platform posed concern over issues of medical confidentiality, protection of patient privacy and data protection of health information and on this basis, violated Article 22 Constitution, Article 8 ECHR, the Directive 95/46/EC, and the 1992 Data Protection Act. In particular, the claimants were concerned about the use and the transfer of sensitive health data via the eHealth platform. In addition, they argued that by using the Belgian national number as a key to access to the health file, a link could be made between personal health information and other data which might interfere with the medical confidentiality.

Contrary to its previous judgment, the Constitutional Court found the action for annulment of the eHealth Act inadmissible. It ruled that the Act, including its provisions on the patient's required consent, met all requirements imposed by the 1992 Data Protection Act, the Constitution and the international obligations.[55] It underlined that the eHealth platform had been created to provide a secure exchange of existing data. The platform was in principle not authorised to collect new health data, nor to store this data.[56] Quoting from the parliamentary proceedings, the Court also found that the objectives and tasks of this platform were defined and explained in a detailed and precise manner. With regard to the use of citizens' national number as a key to the system, the Court decided that, given the confidentiality safeguards included in the Act of 21 August 2008, the use of a unique national number to access to health information was reasonably justified.[57]

51 Ronny Saelens, 'Vademecum Sociale Media & Arbeidsrelaties. Juridische omkadering van de controle op het gebruik van sociale netwerksites op het werk' (2014) <http://www.privacycommission.be/sites/privacycommission/files/documents/Vademecum-Sociale-media-Arbeidsrelaties.pdf> accessed 10 April 2015.
52 Ronny Saelens, 'EHealth-platform doorstaat grondwettelijke toets' (2010) P&I, 144.
53 Ronny Saelens, 'EHealth-platform doorstaat grondwettelijke toets' (2010) P&I, 144.
54 CC, No. 15/2008, 14 February 2008. See B. Fonteyn & Ch. Dubois, 'La plate-forme eHealth – Enjeux de santé publique et de sécurité sociale' (2012) 131 Journal des tribunaux (24 November 2012) 769.
55 Ronny Saelens, 'EHealth-platform doorstaat grondwettelijke toets' (2010) P&I, 144.
56 Ronny Saelens, 'EHealth-platform doorstaat grondwettelijke toets' (2010) P&I, 144.
57 Ronny Saelens, 'eHealth-wet: nog enkele onduidelijkheden' *De juristenkrant* (Brussels,12 May 2010) 12-13.

2.2. Workplace environment: monitoring with digital means and social media

The 1992 Data Protection Act applies to the processing and collection of personal data activities in the workplace environment.[58] The Act has been clarified, applied and complemented by Collective Labour Agreement No. 81 relating to the protection of the private life of workers regarding the electronic communications network[59] and by Collective Labour Agreement No. 68 relating to the protection of workers' privacy in relation to the use of surveillance camera in the workplace[60]. Also, in this area there is a role for Article 314***bis*** of the Belgian criminal code, which prohibits all interception of the content of communications by third parties. Equally there is a role for Article 123 of the Act of 13 June 2005 on electronic communication protecting data ***about*** telecommunications.[61] This Act is regularly invoked in front the courts when the litigation concerns social media in the workplace environment.[62] In particular, use is made of Article 124 that criminalises actions by third parties that monitor the existence of telecommunications of others without consent. The following actions are prohibited: 1. with fraudulent intent, taking note of the existence of signs, signals, writings, images, sounds or data of any nature that originate from and are addressed to others (Article 124, 1°); 2. with fraudulent intent, modifying or deleting this information by any technical means or identifying the other persons (Article 124, 2°); 3. intentionally taking note of telecommunication data that relate to other persons (Article 124, 3°); 4. disclosing, using in any way, codifying or destroying the information, identification and data set forth in 1, 2 and 3 above (Article 124, 4°).

Surveillance with hidden cameras in the workplace – Cour de Cassation, 27 February 2001

The ***Cour de Cassation*** examined the issue of the use of digital means (***in casu***, a hidden surveillance camera) in the workplace in the case ***Monsieur C.N. v Leli's World.***[63] The defendant was the owner of a shop ('Leli's World'). He installed a hidden surveillance camera and a microphone to monitor the area around the cash register as he suspected one of his employees of stealing. The Ghent Court of Appeal found the cashier guilty of theft on the basis of witness statements and the recording made by this hidden camera installed around the cash register. The claimant (the employee suspected of stealing) brought a claim against his employer arguing that this latter has violated his right to private life and therefore the illegally obtained evidence needed to be excluded due to it being contrary to Article 8 ECHR, the 1992 Data Protection Act and Article 314***bis*** of the Criminal code relative to the privacy of communications.

In this case, the ***Cour de Cassation*** rejected the appeal lodged against the Ghent Court of

58 See on the legal framework in this area Marc Verdussen & Pierre Joassart (eds) ; La vie privée au travail (Anthemis 2011); R. Robert & K. Rosier, 'Réglementation et contrôle de l'utilisation des technologies de la communication et de l'information sur le lieu de travail' in *Le droit du travail à l'ère du numérique* (Anthemis 2011) 231-359.

59 Collective Labour Convention No.81 (2002) Official Journal, 29 June 2002.

60 Collective Labour Convention No.68 (1995); Karen Rosier & Steve Gilson, *supra* note 42.

61 Official Journal, 20 June 2005. See Paul De Hert & Frederique Van Leeuw, ***Cybercrime Legislation in Belgium***, (2011) Country report of the Cybercrime Section of the IACL Congress in Washington 2010, in E. Dirix & Y-H. Leleu (eds.), ***The Belgian reports at the Congress of Washington of the International Academy of Comparative Law*** (Bruylant, 2011), 867-956, 877.

62 Karen Rosier & Steve Gilson, *supra* note 42, 107.

63 *Cour de Cassation*, No. P.99.0706.N/1, 27 February 2001. Comments on the case can be found in: (2001) Computerrecht 202, annotation by Jos Dumortier; (2001) Vigiles 153, annotation by Paul De Hert; (2001) Rechtskundig Weekblad 1171, annotation by Patrick Humblet. See also Paul De Hert & Serge Gutwirth, 'Cassatie en geheime camera's: meer gaten dan kaas' (2001) Panopticon 309- 318; Paul De Hert, 'De waarde van de wet van 8 december 1992 bij de bewijsbeoordeling in strafzaken' (2002) T. Strafr. 310-317; Olivier De Schutter, 'La protection du travailleur vis-à-vis des nouvelles technologies dans l'emploi' (2003) Rev. trim. dr. h., No. 54, 627-664.

Appeal's judgment. The ***Cour de Cassation*** focused on Article 8 ECHR. It considered that this provision is not absolute and "***does not oppose to the fact that an employer, on the basis of a justified presumption that his worker is involved in criminal offenses, tends to prevent the commission of new reprehensible action by installing surveillance cameras***". Furthermore, the purpose of the filming was legitimate and proportional. Nothing in Article 8(2) of the ECHR obliges the employer to inform beforehand his employees of the measure adopted.[64]

We have already mentioned ***Leli's World*** in our introduction of this contribution. Seemingly, the ***Cour de Cassation*** not only accepts the horizontal effect of the first paragraph of Article 8 ECHR ("***Everyone has the right to respect for his private and family life, his home and his correspondence***"), but also of the second paragraph of the said article. This paragraph contains the criteria (legality, proportionality and legitimacy) under which limitations of privacy are deemed possible. However, the approach is loose, unsystematic and not based on any ECtHR analysis. The requirement of legality or transparency (the employer needs a legal basis or to inform beforehand) is simply not checked, which is a serious flaw in the Court's reasoning.[65]

Equally unsatisfactory is the treatment by the Court of the arguments about a violation of the 1992 Data Protection Act and Article 314***bis*** of the Criminal Code relating to the privacy of communications. The argument about the former is simply disregarded with the observation that the claimant does not give any proof of a violation Data Protection Act,[66] although the judgment opens with a full discussion of the argument of the claimant on this point. What evidence is needed to take data protection serious?

Surveillance with hidden cameras in the workplace – Cour de Cassation, 2 March 2005

In a famous 2005 judgment (the ***Manon*** judgment),[67] - again involving the installation and use of a hidden camera by a shop owner to monitor his employee around the cashier area -, the ***Cour de Cassation*** addressed data protection rules, but rejected them anyway considering that "***the monitoring of a cash register by a video surveillance camera does not imply directly or indirectly***

64 "Attendu que le droit au respect de la vie privée, prévu à l'article 8, alinéa 1er, de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, n'est pas un droit absolu Que cette disposition conventionnelle n'empêche pas que, sur la base d'une présomption légitime de l'implication de son employé dans des infractions commises à son détriment, un employeur prenne des mesures afin de prévenir ou de constater de nouveaux faits punissables au moyen de vidéosurveillance dans un espace accessible au public du magasin qu'il exploite; Que, pour autant qu'elle a pour objectif la dénonciation des faits aux autorités et, partant de cet objectif, qu'elle est adéquate, utile et non excessive, une telle mesure n'implique pas d'ingérence dans l'exercice de ce droit au sens de l'article 8, alinéa 2, de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales; Que l'article 8, alinéa 2, de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, n'implique pas que la mesure ainsi prise doit être préalablement annoncée".

65 Paul De Hert & Mieke Loncke, *supra* note 36, 192.

66 "Attendu que, dans ses conclusions, la demanderesse n'a pas invoqué que la preuve apportée en l'espèce reposait sur une infraction punissable à la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel".

67 *Cour de Cassation*, No. AR P.04.1644, 2 March 2005, (C. t/ S.P.R.L. Le chocolatier Manon). (2005) Computerr. 258, annotated by Barbara Ooms & Patrick Van Eecke; (2005) J.T. 211; (2005) J.L.M.B, 1086 annotated by Marie Beernaert; (2005) Journ. proc. No. 499, 23, annotated by Damien Vandermeersch; (2005) Pas. I, 505, annotated by Damien Vandermeersch; (2005) R.A.B.G. 1161, annotated by Damien Vandermeersch; (2005) Rev. dr. p. 668, annotated by Damien Vandermeersch & Christian De Valkeneer; (2006) Soc. Kron. 10. See also Philippe Toussaint, 'La loi des juges' (2005) Journ. proc. No. 499, 29-31; Marie Beernaert, 'La fin du regime d'exclusion syste´matique des preuves illicitement recueillies par les organes charge´s de l'enquête et des poursuites' (2005) J.L.M.B. 1094-1109; Christian De Valkeneer, 'Que reste-t-il du principe de legalite´ de la preuve? Variations autour de quelques arrets récents de la Cour de cassation' (2005) Rev. dr. p. 685-695; Sidney Berneman, 'Is het ontmaskeren van een dief een schending van de privacy waard? Beschouwingen bij het Winkelkassa- arrest van 2 maart 2005' (2005) R.A.B.G. 1177-1187; Patrick Van Eecke & Barbara Ooms, 'Camerabewaking op de werkplek' (2005) Computerr. 261-263; Serge Gutwirth, Paul De Hert & Ronny Saelens, 'Kan privacy nog? Over de voor- en achterkanten van het privacygrondrecht in België' in Martin De Busscher (eds.), *Kan dit nog? Liber amicorum Rogier de Corte* (Kluwer, 2007) 139-159.

the collection of personal data of the employees, under the 1992 Data Protection Act".[68] The video camera was installed to collect images for evidence purposes (to demonstrate the alleged behaviour of one of his employee in front a court). However, the Court denied the applicability of the data protection principles figuring in the 1992 Data Protection Act and the Collective Labour Agreement No. 68. The finding of the Court that filming a person does not equal the processing of personal data cannot be said to be respectful of data protection rules and the EU dimension and background of the 1992 Data Protection Act (the way of installing a camera or its precise location are irrelevant to determine the scope of this Act). It is, especially when confronted with definitional issues, regrettable that the Court did not consider asking a preliminary question to the Court of Justice of the European Union.

What the Belgian Court ***did*** do was to recall its '***Antigone***' case law[69] regarding the admissibility of illegally obtained evidence. The Court stated that a judge is allowed to use illegally obtained evidence when the illegal act is of a minor nature compared to the first offense that the act of filming enabled to demonstrate.[70] The ***Manon*** decision has been seriously criticised as it appears contradictory to decide that recorded images which had to be produced in order to prove that an employee was stealing, are not to be considered as personal data. ***Manon*** in this regard departs from previous decisions issued by the ***Cour de Cassation*** and lower courts where in similar cases the applicability of the 1992 Data Protection Act and the CCTV No. 68 had been recognised.[71]

Monitoring with social media - Namur Labour Court, 10 January 2010

In a judgment of 10 January 2011,[72] the Namur Labour Court ruled on a dismissal for serious misconduct of a worker who posted comments about a colleague on Facebook, deemed racist and xenophobic by his employer. After having briefly examined the facts in light of Article 124 of the Act of 13 June 2005 on electronic communications[73] (secrecy of electronic communications principle) and the 1992 Data Protection Act, the Tribunal found that the impugned remarks were not of a strictly private and confidential nature to the extent that it is a discussion on an open social media website accessible to staff members. A true legal analysis has not been carried out. The Court basically argues that it is 'public' and therefore not protected and adds that if the plaintiff were right about the protection by the 2005 Act and the Data Protection Act, Antigone would nevertheless allow the Court to use the evidence. Ruling on the admissibility of the evidence, the Tribunal also found that is not inadmissible, for the recipient of such conversation, working at the employer's service, to communicate to the employer the content the post placed on the website, especially as its content is confidential but concerns a conflicting working relationship with another member of staff. However, the Court did not agree with the sanction chosen by

68 *Cour de Cassation*, No. AR P.04.1644, 2 March 2005.
69 *Cour de Cassation*, No P.03.0762.N, 14 October 2003.
70 *Cour de Cassation*, No. AR P.04.1644, 2 March 2005; Karen Rosier & Steve Gilson, *supra* note 42, 107.
71 Tribunal of Liège, 6 March 2007; Cassation Court, 14 October 2003, No P.03.0762.N; Cassation Court, 2 March 2005, No. AR P.04.1644.
72 Namur Labour Court, 10 January 2010, < http://www.diversiteit.be/sites/default/files/legacy_files/Rechtspraak_jurisdiction/discriminatie_discrimination/2012/2011_01_10%20Trib%20%20Trav%20%20Namur.pdf. See, F. Hendrickx, 'Sociale media en privacy in het arbeidsrecht' in X, *Recht in beweging,* (Maklu 2013) 19, 42.
73 Act of July 30, 2013 amending Articles 2, 126 and 145 of the Act of 13 June 2005 on electronic communications and Article 90decies of the Criminal Procedure Code, Official Journal, 23 August 2013, Art. 124. « S›il n›y est pas autorisé par toutes les personnes directement ou indirectement concernées, nul ne peut: 1° prendre intentionnellement connaissance de l›existence d›une information de toute nature transmise par voie de communication électronique et qui ne lui est pas destinée personnellement; 2° identifier intentionnellement les personnes concernées par la transmission de l›information et son contenu; 3° sans préjudice de l›application des articles 122 et 123 prendre connaissance intentionnellement de données en matière de communications électroniques et relatives a une autre personne; 4° modifier, supprimer, révéler, stocker ou faire un usage quelconque de l›information, de l›identification ou des données obtenues intentionnellement ou non ».

the employer: the conduct of the employee justified an intervention and the need to make some clarifications but not a dismissal for serious misconduct.[74]

Monitoring with social media - Brussels Labour Court, 4 March 2010

On 4 March 2010, the Brussels Labour Court also had to speak out on a case of dismissal for serious misconduct.[75] An employee had made some aggressive criticisms of his employer on a Facebook page with the name of the firm that was created by a group of employees of the company. After having recognised the 'public' nature of the conversation placed on Facebook and, in that respect, the non-application of the right to privacy of communication, the Court found that given the circumstances (the author of criticisms did not create the forum, there were only a few messages and he manifestly ignored that the group was open to everyone) the dismissal for misconduct issued by the employer was disproportional.[76] It further stated that "***these criticisms were the expression of deep unease and helplessness with respect to an unfair and intolerable situation perceived as unjust and intolerable***".[77]

The legal reasoning in the judgment is (again) striking superficial: there are human rights involved (privacy and freedom of expression), and labour law obliges the employee to be loyal to the employer, but the case of the employee remains within the limits of the accessible, so no dismissal possible for serious misconduct.[78]

Monitoring with social media - Brussels Labour Court, 3 September 2013

In a 2013 case the Brussels Labour Court examined if an employee of a public listed company who had posted critical and sceptical comments about the company's policy on a public Facebook page was rightly dismissed for serious misconduct.[79] The employee (of course) objected to his dismissal and invoked the right to privacy provided by Article 22 Constitution. The Court emphasised the importance of the distinction between information posted on Facebook pages 'publicly' accessible and the ones published on the pages only accessible to 'friends' as the author's expectations in terms of privacy are different.[80] The Court further stated that if a worker places posts on his/her public page, he/she could expect that 'non-friends' have access to his/her conversation.[81] Accordingly, the Court considered that the worker could not claim that his right to privacy was infringed. The Court, nevertheless, held that the employer had infringed article 124 of the Act of 13 June 2005 on electronic communications (secrecy of electronic communications principle), to the extent that he had intentionally taken notice of information on a Facebook page of the employee without consent. But relying on the ***Antigone*** case law[82] the Court nevertheless

74 Fabienne Rapsaet, 'Facebook: vie privée (partagée) des travailleurs ?' <http://secteurpublic.ifebenelux.com/2014/03/04/facebook-vie-privee-partagee-des-travailleurs/> accessed 20 April 2015 ; Securex, 'Vie privée - L'utilisation des réseaux sociaux par les travailleurs' <http://www.securex.eu/lex-go.nsf/PrintReferences?OpenAgent&Cat2=49~~10&Lang=FR>, accessed 20 April 2015.

75 Brussels Labour Court, 4 March 2010.

76 Fabienne Rapsaet, *supra* note 76; Securex, 'Vie privée - L'utilisation des réseaux sociaux par les travailleurs' <http://www.securex.eu/lex-go.nsf/PrintReferences?OpenAgent&Cat2=49~~10&Lang=FR>, accessed 20 April 2015.

77 Fabienne Rapsaet, *supra* note 76.

78 F. Hendrickx, 'Sociale media en privacy in het arbeidsrecht' in X, *Recht in beweging,* (Maklu 2013) 19, 41.

79 Brussels Labour Court, 3 September 2013. See R. Saelens, *Sociale media en arbeidsrelaties. Juridische omkadering van het gebruik van sociale netwerksites op het werk*, (2013) EMSCO, Synthese Rapport D4.1.3b., 48 (66 p) < http://emsoc.be/wp-content/uploads/2013/11/Sensibilisering_werknemers_D413b.pdf.

80 Fabienne Rapsaet, *supra* note 76; Securex, « Vie privée - L'utilisation des réseaux sociaux par les travailleurs », (accessed on 20 April 2015) http://www.securex.eu/lex-go.nsf/PrintReferences?OpenAgent&Cat2=49~~10&Lang=FR

81 Fabienne Rapsaet, *supra* note 76.

82 Karen Rosier & Steve Gilson, *supra* note 42.

held that the information could be produced as evidence as neither the reliability of evidence nor the right to a fair trial were infringed. Accordingly, the Court confirmed the dismissal for serious misconduct.

Given the growing success of social media, we can expect that the case law related to the use of social media by employees will still evolve in the years ahead. Nevertheless, we can already observe in the above described cases that Belgian courts and tribunals have each time carried out a detailed analysis of the specific circumstances of the case (public nature of criticisms, employees' function, social climate in the company, the aggressive or insulting nature of the criticisms) before issuing their final judgment.[83]

2.3. Surveillance by citizens, secret services and law enforcement authorities

Secret surveillance - Brussels Criminal Court of First Instance, 14 January 2002 and Liège Court of Appeals, 27 June 2003

In two judgments, one by the Brussels Criminal Court of First Instance Brussels (14 January 2002)[84] and one by the Liège Court of Appeals (27 June 2003) [85,] the courts ruled on individual data protection rights and the disclosure on the Internet of recordings obtained via a hidden video camera. In both judgments, careful analysis was made of the data protection duties to inform data subjects and to notify the data protection authority. Both courts also looked at evidence law.

The defendant, an animal rights organisation 'Gaia', used a hidden camera to record evidence of ill treatment of animals at markets in Anderlecht and Ciney which were later disclosed, published and distributed on the Internet. The Brussels Criminal Court decided that the Belgian 1992 Data Protection Act applied as video images of persons must be considered 'personal data'. The Court found that by disclosing and sharing on public websites these recordings, Gaia had violated the 1992 Data Protection Act and Article 8 ECHR. The 2002 judgment went at length to show that Article 9 (obligation to inform the individual concerned), Article 10 (the right to access) and Article 17 (obligation to notify the data protection authority) of the Data Protection Act had been violated.

Regarding the admissibility of evidence, the Court concluded that filming individuals without their knowledge, even in a public place, tarnished the admissibility of evidence. Some commentators noted that the judgment cannot be understood as saying that any evidence obtained by a

83 Fabienne Rapsaet, *supra* note 76. See also F. Hendrickx, 'Sociale media', in F. Hendrickx & C. Engels (eds.), *Arbeidsrecht*, Part II, (die Keure 2015), 425-455; Karen Rosier, 'Chronique de jurisprudence 2012-2014- Usage des technologies de l'information et de la communication dans les relations de travail et droit au respect de la vie privée' (2015), Revue du Droit des Technologies de l'Information, No. 59-60, 71-114. See, more general on dismissal, C. Engels & Y.S. Van Der Sype, *Ontslag wegens dringende reden* (Kluwer 2015) with a full chapter on evidence law. Interesting and announcing our next section is also Labour Tribunal Antwerp (section Mechelen) 13 February 2015 ((2015) Soc.Kron., No. 1, 18; https://lex.be/nl/doc/be/rechtspraak-juridatlocationantwerpen-afdeling-mechelen-2014/juridatjuridictionarbeidsrechtbank-vonnis-13-februari-2015-bejc_2015021310_nl) where the court found the following: "When the presence of a "Track and Trace system" in the vehicle, namely a monitoring system linked to a GPS navigation system, is not mentioned in the work regulations and not indicated to the Commission for the protection of privacy, when documents show that the company also had checks of the movements of the sales representative during the private hours and during the weekends, and the company also does not prove that this system could be disabled, then there is a violation of the privacy of the employee". On the use of private detectives in labour relations: Liege Labour Court, 6 February 2015; Labour Tribunal Brussels, 9 September 2016, No. 2015/AB/624. See Karen Rosier, 'Détectives privés et vie privée: mener l'enquête, mais pas en toute discrétion', *Recueil de jurisprudence du Forum de l'assurance (jurisprudence 2014)*, (Anthemis 2015)

84 Criminal Court of First Instance Brussels, 14 January 2002.

85 Liège Court of Appeals, 27 June 2003.

civilian party using a hidden camera will be always considered as inadmissible.[86] In this particular case, the evidence was rejected because of Gaia's behaviour towards the court (contempt of court) and Gaia's loyalty towards the witnesses.[87]

Seized for a similar case, the Liège Court of Appeal considered that "***the claim of an individual to respect for his private life is assessed less strictly as tapes are recorded in a public place where defendants could be seen everywhere***".[88] The Court also further recalls that "***citizens and public authorities are subject to Article 8 of the Convention [...] an interference may come from a private person, in exceptional circumstances, 'only if it is strictly necessary, having weighed on one hand, the need to protect privacy and, on the other hand, the predominant legitimate reason***". Finally, it also stated that "***given the aim pursued by Gaia, the measure appears adequate, relevant and not excessive***".[89]

The outcome of the case stands in striking contrast with the outcome of the case brought before the Brussels Criminal Court discussed ***above***. While the Brussels court has given a strict interpretation to the right to privacy and the rules of the 1992 Data Protection Act, the Liège court applied a loose proportionality test solely based on Article 8 ECHR, ignoring (better: not applying properly) the data protection rules in the 1992 Data Protection Act, simply concluding that individuals have less privacy in public places.

None of the judges in either case seriously examined the 1995 European Directive and the 1992 Data Protection Act with regard to the processing of data for the purpose of journalistic activities. Both texts foresee an exception to the data protection duties for these kinds of activities. We believe that if the Brussels Criminal Court had read about this exception in more detail, then the case could have been approached from a different perspective. Undeniably the animal activists were not members of the press, but the purpose of their actions could have been labelled as such.

Surveillance of a street by private individuals - Cour de Cassation, 5 June 2012

In a judgment of 5 June 2012,[90] the ***Cour de Cassation*** had to deal with a case concerning the installation and use of a hidden surveillance camera by private individuals. The defendants were a couple that had installed in 2006 a hidden surveillance camera on their balcony in order to monitor their own cars that had on several occasions been subject to vandalism. This surveillance camera recorded a man (the claimant) puncturing the tyres of the defendants' car. The footage was disclosed to the police in order to open an investigation. The claimant challenged the admissibility of the evidence according to Article 6 ECHR (respect for the rights of the defence). Furthermore, he based his complaint on the violation of his rights to privacy and to protection of his personal data under Article 8 ECHR and several provisions of the 1992 Data Protection Act.

In relation to the rights to privacy and to protection of personal data, the ***Cour de Cassation***

86 Olivier Leroux & Yves Poullet, 'Note - En marge de l'affaire Gaia de la recevabilité de la preuve pénale et du respect de la vie privée' (2003) Tijdschrift voor Belgisch Burgerlijk Recht, 163-176.
87 Olivier Leroux & Yves Poullet, *supra* note 88.
88 Olivier Leroux & Yves Poullet, *supra* note 88.
89 Olivier Leroux & Yves Poullet, *supra* note 88.
90 *Cour de Cassation*, No. P.11.2100.N, 5 June 2012. See Ronny Saelens, 'Arrest van het Hof van Cassatie van 5 juni 2012. Verborgen camera is niet verboden voor vaststelling vandalisme' in X, *Praktijkgids Cameratoezicht* (Politeia 2012) 51-53.

applied the 'Antigone test' and found that the violation of the right to privacy is proportionally very low compared to the material damage caused by the claimant. Therefore, the ***Cour de Cassation*** confirmed the decision of the Court of Appeal that there is no violation of privacy according to Article 8 ECHR and the 1992 Data Protection Act and approved the admissibility of the evidence. It further explained its decision by explaining that "***the video camera was positioned looking at the cars so that the interference with the right to privacy of the passers-by was minimal***". It also observed that "***the 1992 Data Protection Act does not provide any sanctions of nullity or sanctions of exclusion of evidence in case of violation***". Finally, it considered that the objective information gleaned from the footage that helped the police to identify the claimant was solely complementary information and not strictly personal data.

This 2012 judgment did not contain any reference to the relevant European law or case law. The ***Cour de Cassation*** did not deny the violation of the 'privacy rights' of the claimants but sees no reason to reject the evidence after balancing all the relevant interests.[91]

Use of Global Positioning System (GPS) by private detectives - Tribunal of Hasselt, 14 June 2011

In a 2011 case, the Tribunal of Hasselt had to rule on the right to protection of personal data and the use, by a private detective, of a GPS-device linked to a computer for private surveillance purposes. [92] The claimant had been tracked by two private detectives (the defendants) through the means of the GPS device installed under her own car and linked to a computer by the detectives. She brought this case in front the Tribunal of Hasselt and claimed that by having used such technology, the private detectives had processed and recorded her personal information without her consent and without any lawful purpose and had violated the 1992 Data Protection Act. The defendants argued that such processing of personal data had been executed under the basis of a lawful interest which is "the marriage settlement" existing between the claimant and their client (the claimant's husband).[93]

The Tribunal reached the conclusion that the defendants, in processing the personal data of the claimant and according to the definitions laid down in Article 1 Data Protection Act did not have any legitimate interest to use such a system of surveillance. It further explained that the private detectives also had not respected the requirements of finality, proportionality and transparency pursuant to Article 4 and 9 Data Protection Act in their processing activities. In its decision, the Tribunal stated that according to the established case law, there exists between spouses a right to healthy curiosity but this right should not be exercised in a disproportionate way. However, ***in casu***, placing a GPS tracking system exceeds the bounds of the right to healthy curiosity.[94] The Court imposed criminal sanctions for unlawful processing based on Article 4 and 9 Data Protection Act.

91 "Par ces motifs, les juges d'appel ont justifié légalement leur décision selon laquelle les images vidéo illégalement recueillies ont certes été obtenues en opposition au droit du demandeur à la vie privée, mais ne doivent pas être écartées des débats en qualité de preuve".

92 Tribunal of Hasselt, 14 June 2011, (2014) *Vigiles* No. 4-5, annotated by Ronny Saelens. See also on the theme of private detectives used by employers, the case law and literature *supra* note 85

93 Furthermore the claimant argued that the defendants have violated Article 5 of the Law of 19 July 1991 on the profession of private detectives stipulating that "*It is forbidden for private detective to spy or to take or to have intentionally taking pictures of people who are in non-public places, through the means of any specific device, without having received their explicit consent for the purposes pursued. It is forbidden for private detectives to install or make available to the customer or any third-party a device with intent to commit one of the acts described in paragraph 1"*

94 Also, the Court observed that the Act of 19 July 1991 regulating the profession of private detectives should be modified in order to comply with the general principles stemming from the 1992 Data Protection Act.

The judgment does not contain a reference to European law or a discussion of the relevant European case law of the ECtHR.

Use of digital means by law enforcement authorities - Cour de Cassation, 17 March 2010

In a judgment of March 17, 2010,[95] the ***Cour de Cassation*** dealt with a case in which a scene of battery and assaults was brought to justice thanks to the evidence of a CCTV camera installed in the street. The plaintiff criticised, before the ***Cour de Cassation,*** Liege's Court of Appeal decision for having refused to exclude the evidence, which, according to him, are in breach of his right to privacy, contained in Article 8 ECHR and of the Articles 4, 5, 8 and 9 Data Protection Act.

The ***Cour de Cassation*** confirmed the Court of Appeal's judgment by considering that the recordings used as evidence did not infringe his right to privacy provided by Article 8 of the EHCR given that "***the mere fact that a surveillance camera visibly installed on the street in order to record evidence of crimes cannot by nature interfere with the right to respect for private life***". Hence, more is needed to create privacy interference in public spaces. This 'more' did not present itself, "***given that the behaviour of the claimant has taken place in the public sphere, the recorded scenes do not interfere with his intimacy***".

The claimant had also invoked breaches of several provisions of the law of 8 December 1992. The answer of the ***Cour de Cassation*** was very brief: 'even in the hypothesis that these provisions are violated, there is no proof by the claimant that this violation meets the ***Antigone*** criteria'.

Again, we are confronted with no references to European case law or law and a court strategy solely based on denying that Article 8 ECHR applies and on accepting the evidence notwithstanding a violation Data Protection Act.

Not long after, in October 2010 the ***Cour de Cassation*** would deal with a similar case:[96] use of images taken from a CCTV camera for the investigation of a crime ('forgery') that was not strictly speaking part of the list of crimes against which the CCTV camera was meant to be used for. This time the analysis concentrated on the provisions of the CCTV Act of 2007 and the Court would reach a similar pragmatic conclusion: images can be used for the investigation of ***all*** crimes. The plaintiff had argued that images taken by a surveillance camera may only be used for the purposes listed in Article 2, 4° of the CCTV Act, which was not the case.[97]

However, the Court decided that, while a surveillance camera may only be installed and used for the purposes listed in Article 2, 4° of the Camera Law, the use of the ***images*** taken by the surveillance camera is not limited to these purposes. According to the Court, Article 2, 4° of the Camera

95 ***Cour de Cassation***, No. C.11.0777.F, 17 March 2010. See P. De Hert & R. Saelens, 'Filmen maar! Versoepeling van de camerawet door het Hof van Cassatie' (2012) 82 ***Rechtskundig Weekblad***, 1332-1333 & 1338-1344. See equally P. De Hert & R. Saelens, 'L'utilisation d'images de caméras comme preuve d'infractions constatées par hasard. Annotation de Cass. 5 octobre 2010' (2011) 17 ***Vigiles. Revue du droit de police***, No. 2, 43-47; Jean-Marc Van Gyseghem, 'Chronique de Jurisprudence' (2012) Revue du droit des technologies de l'information, No. 48-49, 68 and foll.

96 ***Cour de Cassation***, No. C.11.0777,5 October 2010. See P. De Hert & R. Saelens, 'L'utilisation d'images de caméras comme preuve d'infractions constatées par hasard. Annotation de Cass. 5 octobre 2010' (2011) 17 ***Vigiles. Revue du droit de police***, No..2, 43-47 ; Jean-Marc Van Gyseghem, ***supra*** note 95, 68 and foll. ; Van Bael and Bellis 'Belgium: Supreme Court Clarifies Key Concepts of Camera Law' 19 January 2011, http://www.mondaq.com/x/120134/Information+Security+Risk+Management/Supreme+Court+Clarifies+Key+Concepts+of+Camera+Law.

97 This provision defines a "surveillance camera" as an observation system, the purpose of which is to prevent, establish or detect certain criminal offences policed by the municipality or to maintain public order, and which collects, processes or stores images for these purposes.

Law must be read in conjunction with Articles 6, §3 and 9 of the Camera Law which governs the use of the ***images*** taken by a surveillance camera.

We find no difficulty with the October judgment, although the CCTV Act could have benefited from more clarity at this point, clarity that would be given in 2012 with an Act complementing the CCTV Act.[98] The whole issue both in the March and October judgments turns around the principle of purpose limitation, well known in data protection law, but left untouched in both cases.

Use of digital means by law enforcement authorities - Constitutional Court, 22 September 2011

Before the Constitutional Court was brought a request for the annulment of the Act of 4 February 2010 concerning the methods of data collection by intelligence and security services. The request was filed by the Order of Flemish Barristers (***Orde van Vlaamse balies***) and the Flemish Human Rights Organisation (***Liga voor Mensenrechten***).[99] The Act in question amended an Act of 30 November 1998 regulating the powers of the security and intelligence services by adding a number of additional legal methods for collecting personal data, so called special intelligence methods. These powers related, among others, to the possibility to put wire taps on phones, to enter the homes of people suspected of being involved in terrorist activities without them knowing, and/or to detain and question people. [100]

Among other grounds the claimants argued that the newly created investigation measures were particularly invasive and disproportionate in relation to the fundamental rights, including ***inter alia*** the right to a fair trial and the right to privacy. They further argued that the lack of provision for the secret services to inform people of a surveillance measure (Article 2 of the Act) was in breach of Article 8 ECHR, Article 22 Constitution and the 1992 Data Protection Act. They argued that ***"the absence of a compulsory notification duty and the overly restrictive conditions to which the notification is subject do not meet the criteria of "absolute necessity" of Article 8§2 ECHR"***.[101]

The Constitutional Court did not find any violation of Article 8 ECHR in terms of proportionality, which is partly questionable,[102] but it ruled for a partial annulment of the Act with regard to the issue of notification. The original Act did not foresee an active duty to notify ***a posteriori*** the citizens that had been subject to surveillance. At this point the Court found a violation. The Constitutional Court firstly recalled the jurisprudence of the ECtHR by stating that "***the necessity, in accordance with the jurisprudence of the European Court of Human Rights, to inform the person concerned after the termination of investigative measure cannot jeopardise the effectiveness of the method concerned (ECtHR, 29 June 2006, Weber and Saravia v. Germany, § 135; ECtHR, 6 September 1978, Klass and others v. Germany, §§ 57 and 58, ECtHR, 26 March 1987, Leander v. Sweden, § 66)***".[103] In this respect, the Court considered that although it is desirable to inform

98 See F. Schuermans, 'Het gebruik van camera's in de (strafrechts)handhaving: volatiele rechtspraak vraagt en krijgt meer duidelijkheid van de wetgever' (2012) No. 5 Tijdschrift voor Strafrecht 312-319.

99 CC, No. 145/2011, 22 September 2011.

100 See Anne Weyembergh & Céline Cocq, 'Belgium' in Kent Roach (ed.) , ***Comparative Counter-Terrorism Law*** (Cambridge University Press 2015) 234, 249-251.

101 CC, No. 145/2011, 22 September 2011, para A.16. See on this case, Paul De Hert & Franziska Boehm, 'The Rights of Notification after Surveillance is over: Ready for Recognition?' in Jacques Bus (ed.), *Digital Enlightenment Yearbook 2012* (Amsterdam, IOS Press, 2012) 19-39

102 See critically, Tom Decaigny & Paul De Hert, 'De Wet bijzondere methoden inlichtingen- en veiligheidsdiensten (BIM). Het perspectief van de rechten van de verdediging' (2008) 8 No. 1 AdRem. Tweemaandelijks tijdschrift van de Orde van Vlaamse Balies 24-39.

103 CC, No. 145/2011, 22 September 2011.

the person concerned by the investigative measure, there is no constitutional and conventional provision requiring an automatic and compulsory notification. Such notification could, in certain circumstances, jeopardise the finality of the investigative measure concerned and break in a disproportionate way the balance created by the legislator. However, the Court, secondly, decided that Article 2 of the Act did breach Article 8 ECHR, Article 22 Constitution and the 1992 Data Protection Act to the extent that "***it only provides a notification at the request of someone having a legitimate interest, without providing that such notification shall also take place at the initiative of the departments concerned as soon as the Administrative Commission considers that such notification is possible"***.[104] In its view, intelligence services themselves must actively inform the person concerned as soon as it is possible without compromising the intelligence.

Use of data retention by law enforcement authorities - Constitutional Court, 11 June 2015

On 11 June 2015, following two actions for annulment, the Belgian Constitutional Court ruled against the mass collection of communications metadata,[105] in line with the 2014 ***Digital Ireland*** ruling of the Court of Justice of the European Union (CJEU) .[106] This invalidated the Data Retention Directive (2006/24/CE) [107] that inspired the Belgian law.

It can be recalled that the 2006 Directive required telecommunication service providers or operators to retain communications metadata on each and every customer for between 18 months and two years. Belgium was late in adopting a domestic legal instrument to transpose the Directive, partly due to the data protection defects of the Directive, that was by then disapproved of by several national constitutional courts in other countries, were obvious. Finally, in July 2013, the Belgian Federal Parliament adopted, under an emergency procedure, an act and a decree transposing the Directive into Belgian law adding some additional data protection safeguards to the content of the Directive.[108] The amended Belgian Act on Electronic Communications foresaw, for instance, that each police use of metadata is controlled by a magistrate, and, imposes criminal sanctions for access to and use of the retained data for purposes other than those foreseen in the Act.

The emergency procedure did not allow a full parliamentary procedure and was therefore criticised. The outcome, - an amended Belgian Act on Electronic Communications - was also criticized because it went even further in certain respects than what was foreseen in the Directive. For instance, Article 5 of the Belgian Act did not limit the data retention powers to serious crime

104 Jean-Marc Van Gyseghem, *supra* note 97, 68 and foll.

105 CC, No. 84/2015, 11 June 2015.

106 CJEU, Joined Cases C-293/12 and C-594/12, 8 April 2014, *Press and Information Digital Rights Ireland and Seitlinger and Others*. In its 2014 judgment the CJEU declared the 2006 Directive invalid for lack of checks and balances: the wide-ranging and particularly serious interference of the Directive with the fundamental rights at issue was not sufficiently circumscribed to ensure that that interference is actually limited to what is strictly necessary.

107 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54).

108 Act of July 30, 2013 amending Articles 2, 126 and 145 of the Act of 13 June 2005 on electronic communications and Article 90decies of the Criminal Procedure Code, Official Journal, 23 August 2013. See *'New Bill on Data Retention for Telecommunications Operators' Van Bael and Bellis on Belgian Business Law,* Volume 2013, No. 7, 6-7 via http://www.vanbaelbellis.com/en/fiches/publications/newsletters/?Area=237; Jan Dhont & David Dumont, 'Belgium Introduces Broad Data Retention Obligations' http://www.lorenz-law.com/wp-content/uploads/Belgium-Introduces-Broad-Data-Retention-Obligations.pdf.

but allowed use of the data for ***all*** crimes. Moreover, the Act opened up the list of possible governmental agencies that could make use of the data: not only law enforcement authorities but also secret services and certain other services.[109]

In February 2014, several human rights NGO's -***NURPA, datapanik.org,*** the ***Liga voor Mensenrechten*** and the ***Ligue des Droits de l'Homme (LDH***)-, jointly initiated a crowdfunding campaign to finance a claim before the Constitutional Court. [110] The money was quickly raised. The other action for annulment was introduced by the ***Ordre des barreaux francophones et germanophone***. Amongst the sources referred to by the NGO's and the lawyers association are the fundamental rights contained in the ECHR and the EU Charter, the ECtHR privacy case law, the April 2014 judgment by the CJEU and the data retention case law of other national constitutional courts. The ***Liga voor Mensenrechten*** and the ***Ligue des Droits de l'Homme*** concentrated on rights such as privacy, data protection and the presumption of innocence, whereas the ***Ordre des barreaux francophones et germanophone*** focused exclusively on Article 6 ECHR, Article 47 EU Charter (fair trial) and on the need to protect the professional privilege of lawyers.

In its ruling in 2015 the Constitutional Court quoted the April 2014 judgment of the CJEU extensively. It did not focus on the checks and balances that were added by the Belgian legislator to the content of the Directive when drafting the 2013 Act. Rather it found in the Belgian Act the same flaws as those identified by the CJEU: a) the law applies to everyone (without distinction based on the goal of protecting serious crime), including persons that cannot be related to criminal activities and persons that benefit from professional immunities, b) the Act did not focus on data pertaining to a certain period or a specific geographical area; c) no substantive or procedural requirement was built in with regard to the access by the authorities authorised to access the data; d) with regard to the data retention period no distinction was made between the categories of data on the basis of their utility for the objective pursued or on the basis of the persons involved.

On the basis of these findings, the Court found that the amended Act on Electronic Communications violated articles 7 and 8 EU Charter and article 52 Charter (which states that limitations on people's rights are only allowed if they are necessary and genuinely meet the objectives of general interest), and therefore the Constitutional Court concluded that the amended act violated the provisions of Belgian Constitution 'read together with these (EU) provisions'. We paraphrase as much as possible to illustrate the lack of constitutional pride of the Belgian Constitutional Court and its fascination for 'higher' norms: the incompatibility was first found with the provisions of the Charter read in conjunction with the Belgian Constitution and not the other way around.
We note in passing that the ***Ordre des barreaux francophones et germanophone*** initially had invited the Constitutional Court to make use of the preliminary procedure and to ask 'a question' to the CJEU about the compatibility of the Directive with the EU Charter.

109 See Caroline De Geest & Raf Jespers, 'Dataretentie: buitensporig en onevenredig!' (2015) Mo at http://www.mo.be/opinie/dataretentie-buitensporig-en-onevenredig.
110 'Belgian Constitutional Court rules against data retention' (2015) Edri 13.12 i 3.

2.4. Online Marketing

Brussels Court of Appeal, 26 June 2007

The Brussels Court of Appeal in 2007 ruled on the notion of 'personal data'.[111] The claimant in this case brought a claim against a notary for violation of his right to protection of personal data on basis of the 1992 Data Protection Act and Article 8 ECHR. The notary had sent to his clients an email containing a poster with a list of properties for sale and including also properties and names of the neighbours without their consent. The claimant was one of the neighbours. He claimed that the disclosure of his name and address in these emails consisted in "***an unlawful processing of his personal data***" pursuant to Article 3§1 Data Protection Act.

The Brussels Court of Appeal rejected this claim, reaching the conclusion on a double basis: neither 1992 Data Protection Act nor Article 8 ECHR was applicable. To understand the argument about the 1992 Data Protection Act it is useful to recall that the Act applies either when computers are used for data processing or, when this is not the case, data is processed or collected in structured 'files'.[112] The Court did not even consider the first hypothesis and focused on the assumption that no computers were used by the notary in the process: it held that the mere mention of the name of a property owner adjacent to the description of its property on a poster listing properties for sale could not be considered as "***the processing of personal data in a file***" in the sense Data Protection Act.[113] In its argumentation, the court referred firstly to the definition of the term 'file' in the 1992 Data Protection Act and in the 1995 Directive and secondly, to a ***Cour de Cassation*** judgment of 16 May 1997. [114] In our view, the Court missed the point and should have declared the Act applicable under the first hypothesis (computers were used to process the data): the making of the poster and the use of email proves that digital technologies were used.

The other part of the rejection by the Court relates to Article 8 ECHR. The Brussels Court explained that, "***by the fact that the names of the owners were mentioned and not the cadastral data of the property, there is no violation of Article 8 ECHR for the simple reason that these personal data are publicly available for everyone who is interested. Hence, even if these names were not listed on the contested poster, each bidder is able to obtain them***".[115] The argument 'no violation since the data can be found in open registers' is not pertinent since the administrative authorities responsible for these registers can only allow access to data (and thus give the names) when requirements such as 'proportionality' and 'necessity' are met.

111 Brussels Court of Appeals, 26 June 2007. See Jean-Philippe Moiny & Jean-Marc Van Gyseghem, 'Chronique de Jurisprudence' (2009) No.35, R.D.T.I 87; P. De Hert & R. Saelens, "De vermelding van een naam op een verkoopaffiche is geen «verwerking» van «persoonsgegevens"'(2008) 72 No. 14 Rechtskundig Weekblad 578-583.

112 Handwritten and other non-digital files fall under the Act when they are kept in a 'file'. All the rest involving digital technologies, like is the case here, falls under the Act.

113 "Article 1, § 3, Data Protection Act defines a file as 'any set of personal data according to if certain criteria are accessible, whether they are centralized, decentralized or distributed on a functional or geographical organized manner'. According to the *Cour de Cassation* 16 May 1997, there is only a file when the logical structured manner of a set of personal data is compiled and stored and systematic consultation is possible (Cass. May 16, 1997, RW 1997-98, 850)".

114 *Cour de Cassation*, 16 May 1997, (1997) Computerrecht No4, 161-164 annotated by J Dumortier. See J. Buyle, L. Lanoye, Y., Poullet, & A. Willems, 'L'informatique. Chronique de jurisprudence (1987- 1994)' (1996) Journal des tribunaux, 229-251. Also accessible via https://www.law.kuleuven.be/lib/plone/tijdschriften/cassatie/1997/4.pdf.

115 Brussels Court of Appeals, 26 June 2007.

2.5. Online Media

Black listing of sportsmen - Constitutional Court, 19 January 2005

In 2005, the Constitutional Court had to rule on the principle of proportionality in the case ***Monsieur J.V. v Communauté flamande,***[116] stemming from the right to privacy in a case of doping in sport. The claimant was a non-professional cyclist who had used anabolic steroids to improve his sport performances. As a sanction, the Belgian League of Velocipedes imposed upon him a lifetime suspension from all bicycle races and his suspension was published on the official website of the Flemish Community, in accordance with Article 40, Paragraph 6.2 of the Flemish Decree of 27 March 1991.[117] In accordance with this provision the notice published his name, first name, date of birth, the suspension period and the sport he played.[118] Monsieur J. V. requested the annulment of Article 40, Paragraph 6.2 before the Constitutional Court on the grounds that the said Article violated Article 22 Constitution (the right to the respect of private and family life). He argued that the publication of the suspension notice on a website accessible to anyone represented a disproportionate measure which was incompatible with the purpose to inform sports associations about the fact that a certain disciplinary measure had been taken and that they had to implement it.[119] In addition he claimed a violation of the principles of equality and non-discrimination safeguarded respectively by Article 10 and 11 Constitution.[120] The Court decided that "*the publication of disciplinary sanctions against sportsmen on a public website accessible to anyone constituted a violation of the right to respect for private life*". In addition, the Court also underlined that "*the publication was not proportionate with the purpose pursued by the government to inform sports associations, considered that anyone could get these data and process them further even once the website had disappeared. The government's aim could have been reached making the notice accessible to specific organisations only (and not to the wide public), so respecting the claimant's private life*". In accordance, the judges stated that Article 40, paragraph 6.2. of the Flemish Decree infringed Article 22 Constitution and the 1992 Data Protection Act and repealed the pertinent parts of Article 40, Paragraph 6.2 of the Decree.

Defamation - Liege Court of Appeal, 25 November 2008

A 2008 judgment of the Liege Court of Appeals concerned the disclosure of health information about a deceased child, the right to privacy and the medical confidentiality.[121] The claimants were the parents of a deceased child. They brought a claim against two doctors who had held a press conference following the death of their daughter. They argued that the doctors have violated their right to privacy and the obligation, sanctioned by criminal law, to respect medical confidentiality by disclosing to the press health information of their child and the circumstances of their child's death. The Court, without referring explicitly to Article 8 ECHR and Article 22 Constitution, found that there was no violation of the right to privacy: the doctors had only held a press conference

116 CC, No. 16/2005, 19 January 2005. See Antonella Galetta & Paul De Hert, *supra* note 11.
117 Flemish Decree 1991, Art. 40, para 6.2.
118 Flemish Decree 1991, Art. 40, para 6.2.
119 Antonella Galetta & Paul De Hert, *supra* note 11.
120 CC, No. 16/2005, 19 January 2005. See Jean-Philippe Moiny & Jean-Marc Van Gyseghem, 'Chronique de Jurisprudence' (2009) R.D.T.I. No.35, 83.
121 Liege Court of Appeals, 25 November 2008. See R. Saelens & P. De Hert, 'Openbaarmaking van gezondheidsgegevens en het recht op privacy. De toepassing van de bescherming van persoonsgegevens blijft en moeilijke drempel, (annotation of Liège 25 November 2008), (2011) No. 3 Tijdschrift voor Gezondheidsrecht 280-284.

in order to contradict the statements earlier made by the parents to the medias on the incompetence of these doctors having caused the death of their child.[122]
In the judgment, one finds no analysis of the case law of the ECtHR. Equally there is no discussion of impact Data Protection Act.[123]

Defamation - Liège Court of Appeal, 22 October 2009 and Cour de Cassation, 16 June 2011

In ***Test-Achat***, another case related to online media, the Liège Court of Appeal examined the notion of personal data in the digital environment.[124] The claimant had posted defamatory statements about a company (***H. L.***) on the ***Test Achat*** (a Belgian consumer organisation) forum. He opposed H.L.'s obtaining of a judicial order by ***H. L.*** that allowed this firm to access to the identification information registered in the database of ***Test Achat***. The Liège Court of Appeal confirmed the applicability Data Protection Act and stated that "***the identity of the members of a forum as well as the user details (username, etc.) are constitutive of personal data***".[125]. It then considered, after balancing the interests at stake, that the privacy rights of the individual prevailed over the interest of ***H. L.*** and therefore, condemned ***Test-Achat*** to the restitution of 'the user details concerned' to the individual.[126]

The judgment was upheld in 2011 by the ***Cour de Cassation***.[127] This Court concentrated on the 2000 EU e-Commerce Directive and its transposition in Belgium law via the Act of 11 mars 2003 on Act on the Information Society Services. Neither of these instruments contained a 'subjective' right for ***H. L.*** to obtain the data of those who have posted something on websites: "***Article 21,*** § 2 ***of the Act on the Information Society Services does not confer to a person, who alleges being a victim of defamation statements published on a website of a service provider, the right to obtain from the judicial authorities an order to the service provider to communicate all information on the person which has posted this defamation statement in order to bring a trial for compensation***".

122 "Attendu que, de surcroît, les éléments recueillis au dossier répressif démontrent que les termes utilisés par les prévenus lors de la conférence de presse n'ont pas porté atteinte à la vie privée des parties civiles, ces derniers se bornant tout au plus à rectifier certains des affirmations de celles-ci".
123 Jean-Philippe Moiny & Jean-Marc Van Gyseghem, 'Chronique de Jurisprudence' (2009) No.35 R.D.T.I 83.
124 Liège Court of Appeals, 22 October 2009, (2010) No. 38 R.D.T.I. 95. See also on this topic in the context of employment law, See also F. Hendrickx, 'Sociale media', in F. Hendrickx & C. Engels (eds.), *Arbeidsrecht*, Part II, (die Keure 2015), 425-455
125 Liège Court of Appeals, 22 October 2009, (2010) No. 38 R.D.T.I. 95.
126 Jean-Philippe Moiny & Jean-Marc Van Gyseghem, 'Chronique de Jurisprudence' (2012) No. 49 R.D.T.I., 75.
127 *Cour de Cassation*, 16 June 2011, No. C.10.0153.F, (2012) R.D.T.I., No. 47, 69, annotated by H. Jacquemin.. See Jean-Philippe Moiny & Jean-Marc Van Gyseghem, 'Chronique de Jurisprudence' (2012) R.D.T.I., No. 49, 75.

3. Observations

3.1. The Constitutional Court's cosmopolitan, non-patriotic approach

In light of the foregoing analysis of case law described, it can be stated that the Belgian national courts, the ***Cour de Cassation*** as well as the Constitutional Court, regularly rely on domestic provisions combined with Article 8 ECHR. The latter also relied on Article 7 (privacy) and 8 (data protection) EU Charter in its data retention judgment of 11 June 2015 and has referred to EU Directive 95/46/EC.[128]

A distinction between the right to privacy and the right to data protection is ***quasi*** never made in Belgian case law, probably due to the nature of the Constitution as it only mentions the privacy right and, due to unfamiliarity with the distinction. The author of this contribution has criticised this omission in the past, because too often it contributed to rather sloppy analysis of legal issues: the use of a loose proportionality test faking the privacy test ('a limitation of privacy is legitimate when it is proportional') too often allowed Belgian judges to absent from further exploring the impact of the often very precise data protection rights and requirements on certain conflicts.[129]

The Constitutional Court regularly reiterates the parentage of Article 22 Constitution with European standards on the right to privacy and underlines that the interpretations of Article 8 ECHR issued by the ECtHR apply to Article 22 Constitution.[130]

Also present in the Constitutional Court's decisions are references to ECtHR and CJEU case law. For instance, we have seen that the Court relied on the ECtHR case law in its judgement relating to the duty of notification after an investigative measure.[131] This open, cosmopolitan approach contrasts with the lack of mentioning of the ECtHR and CJEU by the ***Cour de Cassation*** and the lower courts.

In our contribution we have tried to show that the 'policy' line of the Belgian Constitutional Court is that of a loyal partner to the European Courts with only rarely an autonomous, daring more personal patriotic accent. Even in its June 2015 data retention ruling the Constitutional Court seems to hide behind the European shoulder and limits itself to largely repeating the arguments of the CJEU. Its 2004 decision on the limitations and scope of Article 29 Constitution, -a provision drafted in absolute terms going beyond the requirements of the ECHR and the EU Charter-, is equally illustrative of a pragmatic policy not to be the best student in the European privacy and data protection classroom.

128 We can find a good example of such reference to the European conventions in the Constitutional Court's 18 March 2010 (*eHealth Platform*). Not only did the judges verify the compliance of the decree contested with the international obligations stemming from the Directive 95/46/EC and the Convention 108 but they further stated that *"these obligations form an indivisible whole of guarantees provided at Article 22 of the Constitution*". See CC, No. 29/2010, 18 March 2010.

129 P. De Hert & S. Gutwirth, 'Cassatie en geheime camera's: meer gaten dan kaas' (2001) Panopticon 309- 318.

130 Jean-Marc, Van Gyseghem, 'Chronique de jurisprudence', (2012) No. 48-49 RDTI 69.

131 CC, No. 145/2011, 22 September 2011.

3.2. Tribalism of the Cour de Cassation and the lower courts

In particular the ***Cour de Cassation*** bears a heavy responsibility in this regard. Almost all its judgments have been criticised for their noncompliance with the European interpretation of the data protection texts. Only some years ago, in its judgment on private individuals filming a street from their balcony (in 2012), the ***Cour de Cassation*** still maintained that images of individuals shot with a CCTV camera should not be considered as personal data, a finding incompatible with the case law of the European Courts and the Article 29 Data Protection Working Party. The latter repeatedly considered that ***"information concerning someone which even in combination with other elements allowing to identify this person must be considered as personal information",*** including footage.[132]

One can equally refer to the judgment of the Brussels Court of Appeal on 26 June 2007 (on a mailing list of a notary with personal data) with interpretations of 'personal data' and 'the right to privacy' in total discontinuity with the one of the ECtHR and the Belgian data protection authority.[133] We recall that the Brussels Court had considered that "***the mere mention of the name of a property owner adjacent to the description of its property on a poster listing properties for sale cannot be considered as 'the processing of personal data in a file' while the European courts would have undoubtedly considered them as personal data***.[134] Finally, although both European Courts have explicitly recognised that health data belong to the core of the right to private life, the Liège Court of Appeal in its judgment of 25 November 2008 did not recognise the application of Article 8 ECHR (and Article 22 Constitution) to health information leaked by the doctors to the media.[135]

Of course there are exceptions, but they were rare.[136] In the past, we have diagnosed this state of things partly through unfamiliarity with a set of rules that is relatively novel from the side of both the barristers pleading before the courts and the members of the courts, and partly as a deliberate 'exit strategy' aimed at keeping the data protection principles and requirements out of the discussion by minimalizing its core notions such as personal data. [137] Once this set of concrete rules and duties are set aside, it is very easy for judges to do some lip-reading to the right of privacy, -a right whose existence cannot be denied not even in Belgium since it is enshrined in the Constitution-, holding that the right is not absolute and that certain interferences are not disproportional since a loose balancing of interests is at stake (***above***).

The lack of openness is not complete,[138] but strikes as particularly provincial in an area governed

132 Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 01248/07/EN WP 136; Joined cases C-141/12 and C-372/12 - *YS and Others* [2014] OJ C-141/12.
133 Brussels Court of Appeals, 26 June 2007.
134 Brussels Court of Appeals, 26 June 2007.
135 Liege Court of Appeals, 25 November 2008.
136 See President Court Brussels 29 June 2007 (2007) Computerrecht 280, annotated by F. Petillion; Brussels Court of Appeal 28 January 2010, (2010) Computerrecht 108, annotated by B. Bruyndonckx (Sabam/Scarlet). In this case a service provider (Scarlet) refused to install filter software to combat violations of copyright. **The Brussels judge turned to the European Court of Justice with a question about the impact of several directives, including the data protection directive, on the case. See ECJ, C-70-10, 24 November 2011 (Scarlet/Sabam) and ECJ, C-360/10, 16 February 2012, (Sabam/Netlog).**
137 Paul De Hert & Mieke Loncke, ***supra*** note 36 167-209.
138 Closer to the truth is to say that the *Cour de Cassation* shows more openness to European developments when it fits its prosecutorial approach. The example that comes to mind is the *Khan* receptiveness with regard to the exclusion of illegally obtained evidence (*above*).

so clearly by EU law and the case law of two European Courts. Every time when the ***Cour de Cassation*** expresses itself about basic context of data protection, one wonders why no use is made of the possibility to make a preliminary reference ruling to the CJEU. A similar remark can be makde about the lower courts: '***Luxembourg? Never heard about it***'

3.3. The dramatic impact of evidence law on privacy protection and data protection

The development of the ***Antigone*** doctrine is more than relevant for our contribution. Recall that in the slipstream of ***Khan***, and beginning with the ***Antigone*** decision of October 14 2003, evidence law in Belgium took a sharp turn: in lieu of a ***prima facie*** prohibition on the use of illicit evidence, the Court substituted a ***prima facie*** authorisation, except in three narrow cases: violation of a formality established 'nullity'; doubts about the reliability of the evidence, or violation of the right to a fair trial.[139]

With this doctrine, the data protection exit strategy discussed (denying that data protection rules exist or apply)) is no longer needed. Courts can now freely acknowledge the applicability Data Protection Act, but disregard any consequence by stating that the violation of the data protection rules has no impact on the fair trial offered to plaintiffs. A good illustration is again the ***Cour de Cassation's*** judgment of 5 June 2012 where the existence and relevance of the 1992 Data Protection Act is recognized, but where the Court refuses to do anything with it since this Act, which does not contain any ***nullities***, does not force courts in an explicit way to exclude evidence when obtained illegally.

In her important study on the exclusionary rule in a global perspective, Jenia Turner contrasts a strong, "majestic" conception of the exclusionary rule in upcoming or new democracies in Europe and elsewhere with a weakened cost-benefit approach in more established democracies.[140] An important shift from a strong rule of law conception of the exclusionary rule has occurred in the U.S. In the past a more robust conception was in place, focusing on the protection of constitutional rights and the integrity of the judicial system. In famous decisions such as ***Boyd v. United States***[141] and ***Mapp v. Ohio***[142] the U.S. Supreme Court emphasised the critical role of the exclusionary rule in giving meaning to constitutional rights. Without it, constitutional rights would be reduced to "a form of words"[143] and "might as well be stricken from the Constitution."[144]

Our discussion of the case law of the ***Cour de Cassation*** and the lower courts shows that non-exclusion has always served a prosecutorial or employer friendly approach. A concern for rendering privacy, data protection and other constitutional rights effective has been absent.

Many reasons can be advanced to account for the developments in Belgium but it is clear that in the aftermath of the ***Dutroux*** (child molester) scandal, in the beginning of the twenty-first century

139 Marie-Aude Beernaert & Philip Traest, ***supra*** note 3, 181.
140 Jenia Iontcheva Turner, ***The Exclusionary Rule as a Symbol of the Rule of Law***, (2014) 67 SMU L. Rev. 821 < h9p://digitalrepository.smu.edu/smulr/vol67/iss4/13.
141 *Boyd v. United States*, 116 U.S. 616 (1886).
142 *Mapp v. Ohio*, 367 U.S. 643 (1961).
143 *Silverthorne Lumber Co. v. United States*, 251 U.S. 385, 392 (1920).
144 *Weeks v. United States*, 232 U.S. 383, 393 (1914).

a feeling was predominant amongst the magistrates that 'something needed to be done' to regain the trust of the citizen in the judicial system and to make sure that criminals would no longer go unpunished due to failures on the prosecutorial side.

This weakened cost-benefit approach got a second boost when the ECtHR in ***Salduz v. Turkey*** (2007) affirmed the principle that confessions by criminals or suspects without access to legal representation are illegal and, hence, that the presence of a solicitor at police interrogations is part of the human rights ***acquis***.[145] The ruling was not met favourably in countries without access to legal representation during police interrogations.[146] Belgium was one of these countries and its first reaction was the denial of the ***Salduz*** dictum ('that only counts for Turkey'), followed in 2011 by a very modest amendment of the legal framework with the aim of conferring the right to access to a lawyer from the first police interrogation only in certain cases, but for instance excluding the right from suspects that are not detained.[147]

Whatever might be the value of the conversion of ***Salduz*** into Belgian law, the fact is that many amongst the law enforcement apparatus felt deprived of an excellent tool to uncover the truth: the presence of a solicitor took away the advantage of confronting an unprepared suspect. As a consequence, more emphasis should be put on other investigative measures to compensate for this. In particular, privacy infringing measures such as data retention and more CCTV come to mind.[148]

In this climate it is naïve to expect Belgian case law to give meaning to rights such as data protection and privacy. A rare exception, with respect to the ***Dutroux-Salduz*** paradigm, is the 2011 judgment by the Hasselt tribunal where the criminal law sanctions foreseen in the 1992 Data Protection Act were applied in a case of secret surveillance through the use of a Global Positioning System (GPS) by private detectives. If it were not for ***Antigone*** the case might have served as a reminder for police officials collecting evidence in violation of the 1992 Data Protection Act, but clearly that opportunity has not presented itself yet.

3.4. Patterns of litigation before the Belgian courts

Given the wide range of issues examined in our jurisprudential analysis, it is not easy to detect patterns of litigants in the privacy field. However, it is noteworthy that several cases involved professional corporations such as doctors, lawyers and notaries as claimants. The Belgian procedural framework discussed in this paper (1995-2015) did not provide litigants with the possibility to resort to 'class-actions'. Therefore neither the human rights NGO's such as ***La Ligue des Droits***

145 ECtHR, No. 36391/02, 26 April 2007, ***Case of Salduz v. Turkey***.

146 Paul De Hert, 'European Human Rights Law and the Regulation of European Criminal Law' (2010) 1 No. 3 New Journal of European Criminal Law, 289-294. See for a comparative analysis Anton Van Kalmthout et al. (eds.), *Pre-trial detention in the European Union* (Wolf Legal Publishers 2009) 174; Taru Spronken et a. (eds.), *EU Procedural rights in criminal proceedings*, (Maklu 2009). See for Belgium: Laurens Van Puyenbroeck, 'Belgium country report' in Ed Cape et al. (eds.), *Effective Criminal Defence in Europe*, (Intersentia 2010) 67-105.

147 Act of 13 August 2011 amending the Criminal Procedure Code and the Law of 20 July 1990 on the preventive detention as to confer certain rights, amongst which the right to consult and be assisted by a lawyer, to each person interrogated and deprived from his freedom, (2011) Official Journal, 5 September 2011. See P. De Hert, T. Decaigny & M. Colette, 'Cinq manquements de la Loi Salduz par rapport à la jurisprudence de la Cour européenne des droits de l'homme et de la future législation européenne en matière de procédure pénale' in F. Goossens, H. Berkmoes, A. Liners, A. Duchatelet & F. Hutsebaut (eds.), *La réglementation Salduz: Théorie et pratique, aujourd'hui et demain*, (Academic and Scientific Publishers 2012) 301-315.

148 The link between *Salduz* and more non-physical means of truth detection is made in F. Schuermans, 'Het gebruik van camera's in de (strafrechts)handhaving: volatiele rechtspraak vraagt en krijgt meer duidelijkheid van de wetgever' (2012) 5 No. 1 Tijdschrift voor Strafrecht 312.

de l'Homme[149] nor the Belgian Data Protection Authority were able to launch civil actions in data protection matters. While this explains the very small amount of case law concerning the rights to privacy and data protection, we can still expect some changes in the future as occurred recently with the newly rewritten Consumer Ac organizing in a general way a possibility for actions for collective redress.[150]

Although relying on European provisions such as Article 8 ECHR and the EU Directive 95/46/EC in their claims and decisions, we have identified very few, if not a single instance of 'strategic' rights-based litigation or advocacy for domestic reform in the arguments of litigants and decisions of the courts.

Before the Constitutional Court the situation is brighter with not only human rights NGO's but also professional organisations such as the Belgium Association of Medical Professionals, the ***Ordre des barreaux francophones et germanophone*** and the Flemish ***Orde van Vlaamse Balies*** playing an important and often complementary role. The latter successfully focused on fair trial rights in privacy and data protection related issues. In a country with a mediocre constitutional culture regarding privacy and data protection, that might be a very productive approach to prevent these rights from becoming fully reduced to a form of words although they figure prominently in the Constitution and the primary European texts.

The human rights NGOs on both sides of the language frontier in Belgium have rightly prioritised privacy in the recent years. In a commentary on the victory before the Constitutional Court on the data retention powers, Alexis Deswaef, president of ***La Ligue des Droits de l'Homme*** said:

> "*This constitutional ruling should have the effect of a shock to our governments: they cannot expand indefinitely the massive surveillance of their citizens. There is an increasingly obvious imbalance between the respect for privacy and the legitimate need for security. This is what prompted LDH to make data protection and privacy our main themes for 2015*".[151]

3.5. Conclusions: Towards a better culture of respecting both privacy and data protection?

In ***Democracy in Europe***, Larry Siedentop critically diagnoses smaller regions in Europe where, due to historical factors, loyalties to the rule of law and democratic principles are not as closely observed as they ought to be.[152] Our overview of Belgian case law points towards a lack of constitutionalism. Belgium, where the judiciary is today organised in regional units, seems to be simply too small to generate a certain distance needed to 'play the constitutional game'. Magistrates

149 Human Rights association also specialised in privacy and data protection matters.

150 Act of 28 March 2014 concerning an action for collective redress, Official Journal, 2014, 35201. See Janek Tomasz Nowak, 'The New Belgian Law on Consumer Collective Redress and Compliance with EU Law Requirements' in Eva Lein, Duncan Fairgrieve, Marta Otero Crespo & Vincent Smith, *Collective Redress in Europe. Why and How?* (BIICL, 2015) 169-201. See on the potential of this procedure for data protection litigation, Y.S. Van Der Sype, W. Vandenbussche, I. Samyn & N. Portugaels, "Allen tegen één: Over de rechtsvordering tot collectief herstel en de bescherming van persoonsgegevens op het internet', (2014) Computerrecht, No. 6, 315-324.

151 Belgian Constitutional Court rules against data retention' (2015) 13.12 *EDRi-gram* sub 3.

152 Larry Siedentop, ***Democracy in Europe***, (Penguin 2000) 174-176.

in courts, prosecutors, police and policy leaders seem to cross paths regularly and to share a set of implicit values and understandings. At these encounters there is no 'impartial spectator' as proposed by Amartya Sen.[153] Particularly lacking is the ***Eurocrat***. Although 'Brussels' is not far from Belgium politics it would help to make ties stronger. Attempts such as the one by the ***Ordre des barreaux francophones et germanophone*** in the data retention case to ask explicitly for a preliminary procedure to involve the CJEU (***above***), need to be followed. A recent judgment of the CJEU underlines the duties of national courts to identify, of their own accord, the EU law aspects in cases before them.[154] The CJEU replied positively to the question brought before it by a Dutch Court whether a national court before which an action is brought is required to examine of its own accord whether the purchaser is to be regarded as a consumer within the meaning of the Directive, regardless of whether the party has relied on that status. In the view of the CJEU the EU consumer protection system established by Directive 1999/44/EC of 25 May 1999 on certain aspects of the sale of consumer [155] is predicated on the weak position of the consumer ***vis-à-vis*** the seller both in terms of bargaining power and level of knowledge. Accordingly, there is a substantial risk that the consumer, given his lack of awareness, will not rely on the rules that are intended to protect him. A similar reasoning could be built up with regard to data protection law and would, at least in Belgium, contribute to a better culture of respecting both privacy and data protection.

153 Amartya Sen, *The Idea of Justice* (Harvard University Press 2009).

154 CJEU, Case C-497/13, 4 June 2015, ***Froukje Faber v. Autobedrijf Hazet Ochten BV***. See 'CJ Clarifies Consumer Protection Rules Relating to Sale of Consumer Goods and Associated Guarantees' (2015) No. 7, Van Bael and Bellis on Belgian Business Law, 5-6 via http://www.vanbaelbellis.com/en/fiches/publications/newsletters/?Area=237.

155 Directive 1999/44/EC of 25 May 1999 on certain aspects of the sale of consumer, O.J. L 171, 7 July 1999.

The Brussels Privacy Hub Working Papers series

N°1 "The data protection regime applying to the inter-agency cooperation and future architecture of the EU criminal justice and law enforcement area" (November 2014) by Paul De Hert and Vagelis Papakonstantinou (35 pages)

N°2 "The new cloud computing ISO/IEC 27018 standard through the lens of the EU legislation on data protection" (November 2014) by Paul de Hert, Vagelis Papakonstantinou, Irene Kamara (25 pages)

N°3 "Towards efficient cooperation between supervisory authorities in the area of data privacy law" (October 2015) by Dariusz Kloza, Antonella Galetta (24 pages)

N°4 "The data protection regime in China" (November 2015) by Paul De Hert and Vagelis Papakonstantinou (30 pages)

N°5 "The right to privacy and personal data protection in Brazil: time for internet privacy rights?" (February 2016) by Vinícius Borges Fortes (23 pages)

N°6 "Permissions and Prohibitions in Data Protection Jurisdiction" (May 2016) by Mistale Taylor (25 pages)

N°7 "Structure and Enforcement of Data Privacy Law in South Korea" (October 2016) by Haksoo Ko, John Leitner, Eunsoo Kim and Jong-Gu Jung (20 pages)

N°8 "The "Right to be Forgotten" and Search Engine Liability" (December 2016) by Hiroshi Miyashita (15 pages)

N°9 "European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards "Good Enough" Oversight, Preferably but Not Necessarily by Judges" (March 2017) by Gianclaudio Malgieri & Paul De Hert (25 pages)

N°10 "Does Technology Drive Law? The Dilemma of Technological Exceptionalism in Cyberlaw" (July 2017) by Meg Leta Jones, JD, PhD (31 pages)

N°11 "The Microsoft Ireland case and the cyberspace sovereignty trilemma. Post-territorial technologies and companies question territorial state sovereignty and regulatory state monopolies" (July 2018) by Paul De Hert and Johannes Thumfart (27 pages)

N°12 "Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach" (August 2018) by Irene Kamara and Paul De Hert (35 pages)

N°13 "Big data analytics by telecommuni-cations operators and the draft ePrivacy Regulation" (September 2018) by Vagelis Papakonstantinou & Paul de Hert (14 pages)

N°14 "Enforcement in Indonesia Data Privacy Laws: The 2018 Facebook-Cambridge Analytica scandal as a case study" (October 2018) by Anbar Jayadi (21 pages)

N°15 "Belgium, Courts, Privacy and Data Protection. An inventory of Belgian case law from the pre-GDPR regime (1995-2015)." (January 2019) by Paul De Hert (34 pages)

The Brussels Privacy Hub Working Papers series

The Brussels Privacy Hub Working Papers are intended to circulate research in progress for comment and discussion. The Working Papers focus on all areas of data protection and privacy research and can contain empirical research on privacy issues and analytical work on privacy governance and regulation in the EU; global flows of data; reconciling law enforcement and privacy interests; privacy challenges posed by new technologies; comparative research on privacy in different regions; jurisprudential issues of privacy protection; and many others

Available at www.brusselsprivacyhub.org/publications.html

Contact: info@brusselsprivacyhub.eu

See list on previous page