Case Law Overview
1 December 2014 - 31 December 2015

Working Document

Relevant case-law of CJEU, ECHR and national courts of EU Member States on the right to the protection of personal data, the right to the protection of private life, access to documents and the right to freedom of expression. Includes reference to pending cases.

DISCLAIMER

This is an internal working document prepared by the EDPS 'Policy and Consultation' and 'Supervision and Enforcement' Units intended to provide factual summaries of case law. The EDPS relied on the accuracy of data as made publicly available by the relevant Courts. Any commentary or opinion contained therein does not represent the official position of the EDPS.

European Data Protection Supervisor

15 March 2016

TABLE OF CONTENT

I. JUDGMENTS OF THE COURT OF JUSTICE OF THE EUROPEAN UNION

DATA PROTECTION

1) C-212/13, *František Ryneš v. Úřad pro ochranu osobních údajů*, 11 December 2014 - Concept of 'in the course of a purely personal or household activity'

Link

Facts of the case

In 2007**,** Mr Rynes, a Czech citizen, installed a camera system under the eaves of his family home in order to protect the property, health and life of his family and himself. Mr Rynes and his family had been subject to several attacks by persons unknown whom it had not been possible to identify. The device recorded the entrance to his home, the public footpath and the entrance to the house opposite. On 7 October 2007, one of the windows of Mr Rynes's home was broken and the video surveillance system made it possible to identify two suspects against whom criminal proceedings were subsequently brought.

By a decision of August, Úřad pro ochranu osobních údajů, i.e. the Office for Personal Data Protection in Czech Republic, found that Mr Rynes had infringed the Czech Law because he had used a camera system to collect the personal data of persons moving along the street or entering the house opposite (1) without their consent, (2) without informing them at all and, (3) as a data controller, he had not fulfilled his obligation to report that processing to the Office. Mr Rynes challenged this decision in court. The Nejvyssi spravni, the appealing court, lodged a request for a preliminary ruling to the ECJ on 20 March 2013 in order to determine if such use of a camera system amounts to the processing of data in the course of *"a purely personal or household activity"* for the purposes of Article 3(2) of Directive 95/46, and consequently escape the application of Directive 95/46.

Main findings of the Court

- The Court first stated that **the exception** provided for in the second indent of Article 3(2) **must be narrowly construed:** The Court departs from the consideration that the protection of the fundamental right to private life guaranteed under Article 7 of the Charter requires that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary. "*Since the provisions of Directive 95/46, in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must necessarily be interpreted in the light of the fundamental rights set out in the Charter (see Google Spain and Google, EU:C:2014:317, paragraph 68), the exception provided for in the second indent of Article 3(2) of that directive must be narrowly construed."*
- This also appears from the very wording of that provision, under which the directive does not cover the processing of data where the activity in the course of which that processing is carried out is a **'purely'** personal household activity. In that respect, correspondence and the keeping of address books by individuals constitute, in the light of recital 12 to

Directive 95/46, a 'purely personal or household activity' even if they incidentally concern or may concern the private life of other persons.

- However, the Court found that to the extent that video surveillance such as that at issue in the main proceedings covers, even partially, a public space and is accordingly directed outwards from the private setting of the person processing the data in that manner, it cannot be regarded as an activity which is a purely 'personal or household' activity for the purposes of the second indent of Article 3(2) of Directive 95/46.
- The Court ruled that *"The second indent of Article 3(2) of Directive 95/46/EC (...) must be interpreted as meaning that the operation of a camera system, as a result of which a video recording of people is stored on a continuous recording device such as a hard disk drive, installed by an individual on his family home for the purposes of protecting the property, health and life of the home owners,* ***but which also monitors a public space, does not amount to the processing of data in the course of a purely personal or household activity,*** *for the purposes of that provision."*
- The Court specified that *"the application of Directive 95/46 makes it possible, where appropriate, to take into account — in accordance, in particular, with Articles 7(f), 11(2), and 13(1)(d) and (g) of that directive — legitimate interests pursued by the controller, such as the protection of the property, health and life of his family and himself, as in the case in the main proceedings".*

2) C‑446/12 to C‑449/12, *W.P. Willems v. Burgemeester van Nuth, H.J. Kooistra v. Burgemeester van Skarsterlân, M. Roest v. Burgemeester van Amsterdam and L.J.A. van Luijk v. Burgemeester van Den Haag*, 16 April 2015 - Biometric data and purpose limitation

Link

Facts of the case

Mr Willems, Ms Roest and Ms van Luik each made passport applications that were rejected because they refused to provide fingerprints, while Mr Kooistra was denied a Netherlands identity card because he refused to provide fingerprints and a facial image. The applicants refused to provide their biometric data on the ground that it would constitute a serious breach of their right to privacy. They all brought legal actions against the rejection decisions of the Burgemeesters, which they lost, and then appealed before the referring court.

The Raad van State decided to request for a preliminary ruling from the ECJ concerning the interpretation of Articles 1(3) and 4(3) of Council Regulation (EC) n° 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States ('the Regulation').

Article 1(3) of the Regulation states that *"This Regulation applies to passports and travel documents issued by Member States. It does not apply to identity cards issued by Member States to their nationals* ***or*** *to temporary passports and travel documents having a validity of 12 months or less."*

Article 4(3) of the Regulation states that *"Biometric data shall be collected and stored in the storage medium of passports and travel documents with a view to issuing such documents. For the purpose of this Regulation the biometric features in passports and travel documents shall only be used for verifying: the authenticity of the passport or travel document; the*

identity of the holder by means of directly available comparable features when the passport or travel document is required to be produced by law."

Main findings of the Court

- Regarding the interpretation of Article 1(3), it had to be established first if it should be interpreted as meaning that Regulation (EC) n° 2252/2004 is not applicable to identity cards issued by a Member State to its nationals irrespective of the period of their validity, i.e. if the scope of Regulation (EC) n° 2252/2004 varies according to the period of validity of an identity card. In this regard, the Court clarified that *"identity cards issued by Member States to their nationals"* and "*temporary passports and travel documents having a validity of 12 months or less"* were two separate categories of documents since they were connected in the text by the conjunction *"or"*. Therefore, the expressions *"temporary"* and *"having a validity of 12 months or less"* do not concern identity cards issued by Member States to their nationals and those are not in the scope of Regulation (EC) n° 2252/2004 whatever the period of their validity is.
- Second, it had to be established whether the fact that identity cards may be used for the purposes of travel within the EU and to certain non-Member States may bring them within the scope of Regulation (EC) n° 2252/2004. The Court used the same reasoning to conclude that no, that fact does not bring identity cards within the scope of Regulation (EC) n° 2252/2004.
- Regarding the interpretation of Article 4(3) of Regulation (EC) n° 2252/2004, it had to be established if this Article, read together with Articles 6 and 7 of Directive 95/46 and Articles 7 and 8 of the Charter[1], should be interpreted as meaning that it requires Member States to guarantee that the biometric data collected and stored pursuant to that Regulation will not be collected, processed and used for purposes other than the issue of passports or other travel documents. The Court concluded that no, Member States do not have to provide such guarantee in their legislation, since that is not a matter which falls within the scope of Regulation (EC) n° 2252/2004.

3) C-580/13, *Coty Germany GmbH v. Stadtsparkasse Magdeburg*, 16 July 2015 - right to information in the context of proceedings for infringement of an intellectual property right and banking secrecy

Facts of the case

Coty Germany produces and distributes perfumes and holds an exclusive licence for the Community trade mark 'Davidoff Hot Water' for perfumery. Coty Germany purchased a bottle of perfume bearing the trade mark Davidoff Hot Water on an Internet auction platform, and paid the price of that bottle into a bank account opened with the Stadtsparkasse banking institution. Coty Germany found out that the perfume was a counterfeit product and therefore asked the Stadtsparkasse for the name and address of the holder of the bank account. However, the Stadtsparkasse refused to provide this information invoking banking secrecy.

Coty Germany brought an action before the Regional Court, which ordered the bank to disclose the information. The Regional Appeal Court then quashed that judgment invoking

[1]In its judgment in *Schwarz* (C-291/12), the Court already concluded that the use and storage of biometric data for the purposes specified in Article 4(3) of that Regulation are compatible with the requirements of Articles 7 and 8 of the Charter.

that the request of providing information was not justified under the German Law on Trade Marks. Coty Germany appealed then to the German Federal Court of Justice, which lodged a request for a preliminary ruling to the CJEU regarding the interpretation of Article 8(3)(e) of Directive 2004/48 on the enforcement of intellectual property rights, read in conjunction with Article 8(1)(c) of the same text.

Legal Text

According to Article 8(1)(c) of Directive 2004/48, *"Member States shall ensure that, in the context of proceedings concerning an infringement of an intellectual property right and in response to a justified and proportionate request of the claimant, the competent judicial authorities may order that information on the origin and distribution networks of the goods or services which infringe an intellectual property right be provided by the infringer (...)."*

Article 8(3)(e) states that Article 8(1) applies "*without prejudice to other statutory provisions which (...) govern the protection of confidentiality of information sources or the processing of personal data"*.

Main findings of the Court

- **The communication of the name and address of a banking institution's costumer constitutes**, in the view of the Court, **a processing of personal data** as defined in Article 2(a) and (b) of Directive 95/46. (par. 26).
- Article 8(1)(c) and Article 8(3)(e) of Directive 2004/48 read together require that various rights be complied with and reconciled: on the one hand the right to information, which in this case is intended to implement the fundamental right to an effective remedy concerning the infringement of Coty Germany's right to property and, on the other hand, the right to protection of personal data. From Article 2(3)(a) of Directive 2004/48, it is clear that the protection of intellectual property cannot affect the protection of personal data and Directive 95/46. (par. 28-33)
- The Court reminded that *"EU law requires that, **when transposing directives, the Member States take care to rely on an interpretation of them which allows a fair balance to be struck between the various fundamental rights protected by the EU legal order**. Subsequently, when implementing the measures transposing those directives, the authorities and courts of the Member States must (...) make sure that they do not rely on an interpretation of them which would be in conflict with those fundamental rights or with the other general principles of EU law."*(par.34)
- The Court argued that the provision of German Law transposing Article 8(3)(e) allows for an unlimited refusal, as its wording does not contain any condition or qualification. Therefore, such a provision does frustrate the right to information and ultimately the rights to an effective remedy and to intellectual property enjoyed by the holders of these rights. (par. 37-41)
- The Court found that *"Article 8(3)(e) of Directive 2004/48/EC must be interpreted as precluding a national provision, such as that at issue in the main proceedings, which allows, in an unlimited and unconditional manner, a banking institution to invoke banking secrecy in order to refuse to provide, pursuant to Article 8(1)(c) of that directive, information concerning the name and address of an account holder"*.

4) C-363/14, *EP v Council*, 10 September 2015 - lawfulness of an implementing decision amending the list of third States with which Europol must conclude agreements

Link

Facts of the case

The European Parliament brought proceedings for annulment of the Council Implementing Decision 2014/269 amending Decision 2009/935 which determines the list of third States and organisations with which Europol shall conclude agreements.

Main findings of the Court

1) The choice of legal basis

Choice of a repealed legal basis

- The Parliament argued that the Council relied on a repealed legal basis, namely Article 34(2)(c) EU (paras 18-20). The Court held that the Decision does not refer to this legal basis and that the recitals refer to Articles 26(1)(a) of the Europol Decision and Articles 5 and 6 of Decision 2009/934 adopting the implementing rules governing Europol's relations with partners (para 23). Although Articles 5 and 6 do not constitute a valid legal basis, the Court established that this had no effect "on the content of the decision or the procedure for its adoption" (para 27).

Choice of an invalid legal basis

- Alternatively, the Parliament argued that Article 26(1)(a) of the Europol Decision does not constitute a valid legal basis (para 30) because the procedure it provides for amending the list does not follow the procedure established in the Treaties (para 45).
- The Court reiterated that only the Treaties can amend the decision-making procedure set out in them. The fact that "an institution can establish secondary legal bases for the adoption of legislative acts or implementing measures" amounts to "according that institution a legislative power which exceeds that provided for by the Treaties" (para 43).

A) Whether an amendment to the list constitutes an essential element

- The Court stated that "*the provisions laying down the essential elements of the basic legislation, the adoption of which requires political choices falling within the responsibilities of the EU legislature, cannot be delegated or appear in implementing acts''* (para 46). However, the Court found that establishing relations was ancillary to the activities of Europol (para 49) and that amending the list did not require political choices to be made by the legislators (para 51).
- The fact that an amendment **''is liable to have serious consequences for the fundamental rights of citizens cannot change that analysis''** (para 52).
- Nonetheless, the Court acknowledged that the transmission of personal data **''may interfere with the fundamental rights of the persons concerned, and some of**

those interferences may be so serious that intervention by the EU legislature becomes necessary'' (para 53).

- However, the principle of the transmission of personal data to third States and the relevant framework were set by the legislature in the Europol Decision, in particular with regard to the assessment of the adequacy of the level of data protection ensured by the third State concerned' (para 54).
- Moreover, adding a third State to the list does not automatically allow for the transmission of personal data because Europol and the third State must first conclude an agreement authorising such transfer. The conclusion of this agreement requires decisions made by the Europol Management Board, the Council and the Director of Europol (para 55).
- Finally, the Court found that Article 23(1) defines "sufficiently precisely" the conditions to be satisfied before a third State can be put on the list (para 56).
- In conclusion, an implementing act can amend the list because it does not constitute an essential element (para 57).

B) Whether any prior initiative of a Member State or the Commission is required

- The Parliament argued that the procedure is unlawful because it does not require any prior initiative of a Member State or the Commission. The Court held that this must be assessed in light of the provisions which governed implementing acts in the field of police and judicial cooperation in criminal matters when the decision was adopted (para 59).
- The wording of Articles 34(2)(c) EU indicates that an initiative of a Member State or the Commission is necessary for the basic acts that the Council may adopt unanimously but it is not necessary for the adoption of implementing acts (paras 63-65). Moreover, the provisions which entered into force after the Lisbon Treaty do not require an initiative of a Member State or the Commission for implementing measures either (para 66).
- In conclusion, a prior initiative is not necessary and Article 26(1)(a) cannot be considered unlawful on that ground (para 67).

C) Whether the Treaty of Lisbon applies

- The Parliament argued that Article 26(1)(a) of the Europol Decision is incompatible with the procedure set out in the Treaty of Lisbon (para 68).
- The Court stated that Article 9 of the Protocol on transitional provisions "must be interpreted as meaning that a provision of an act duly adopted on the basis of the EU Treaty before the entry into force of the Treaty of Lisbon (...) continues to produce its legal effects until it is repealed, annulled or amended, and permits the adoption of implementing measures in accordance with the procedure it defines" (para 70).
- In conclusion, Article 26(1)(a) cannot be incompatible as the Treaty of Lisbon does not apply (para 70).

2) Breach of an essential procedural requirement

A) No prior initiative

- The Court noted that Articles 26(1)(a) does not require a prior initiative before adopting an implementing decision and the legislative framework applicable at the time, namely Article 34(2)(c) EU, did not require it either (paras 79-80). Therefore, the lack of an initiative does not breach an essential procedural requirement (para 81).

B) Consultation of the Parliament

- The Court recalled that "due consultation of the Parliament" is an essential procedural requirement, "disregard of which renders the act concerned void" (para 82). Articles 26(1)(a) requires the Parliament to be consulted and this is not affected by the changes brought by the Lisbon Treaty (paras 84-86).
- The Parliament argued that an essential procedural requirement had been breached because the Council consulted it without being aware that it was obliged to do so (paras 87-88). However, the Court held that it was not shown that this error prevented the effective participation of the Parliament or that it interfered with the conditions to perform its duties (para 91).
- The Court distinguished the present case from the case C-316/91 *Parliament v Council*, where the Parliament's right to be consulted was infringed despite the fact that an optional consultation took place (para 93) because this issue was only assessed in the context of admissibility and the Court did not rule on whether this constituted an essential procedural requirement (para 94).
- Moreover, the Court has already held that "the incorrect substitution of a legal basis requiring the Parliament to be consulted for a legal basis not requiring such consultation was a purely formal defect" (para 96).

Conclusion: The pleas put forward by the Parliament are rejected.

5) Case C-201/14*, Smaranda Bara and Others v Președintele Casei Naționale de Asigurări de Sănătate and Others*, 1 October 2015 – transfer of personal data between public administrative bodies and subsequent processing without informing the data subjects

Link

Facts of the case

Romanian law allows public bodies to transfer personal data to the health insurance funds for the purpose of determining whether an individual qualifies as an insured person and an internal protocol specifies that this includes income data. The National Tax Administration Agency (ANAF) transferred the applicants' income data to the National Health Insurance Fund (CNAS). The CNAS relied on that data to require payment of arrears of contributions to the health insurance regime. The applicants brought an appeal before the Court of Appeal in which they challenged the lawfulness of the transfer of tax data relating to their income in light of Directive 95/46. In that context, the national court filed a request for a preliminary ruling to establish whether the processing required prior information to be given to the data subjects and whether the transfer of data on the basis of the Protocol is contrary to Directive 95/46.

Main findings of the Court

- The Court summarized the question referred as follows: "the referring court asks, in essence, whether Articles 10, 11 and 13 of Directive 95/46 must be interpreted as precluding national measures, such as those at issue in the main proceedings, which allow a public administrative body in a Member State to transfer personal data to another public administrative body and their subsequent processing, without the data subjects being informed of that transfer and processing" (para. 28).

Applicability of the Directive

- The Court first established that:
  (1) the tax data transferred to the CNAS by the ANAF constitute personal data within the meaning of Article 2(a) of the directive because they are "information relating to an identified or identifiable natural person";
  (2) the transfer of the data and their subsequent processing constitute "processing of personal data" within the meaning of Article 2(b) of the directive (para. 29).

The transfer does not comply with Article 10

- The Court explained that the requirement of fair processing found in Article 6 of the directive "requires a public administrative body to inform the data subjects of the transfer of those data to another public administrative body for the purpose of their processing by the latter in its capacity as recipient of those data" (para. 34).
- In light of the facts of the case, the Court noted that the applicants were not informed of the transfer (para. 35).
- The Court acknowledged that the applicable Romanian law allows public bodies to transfer "the data necessary to certify that the person concerned qualifies as an insured person" to the health insurance funds. Nonetheless, the Court noted that a taxable income is not required to qualify as insured therefore it considered that income data is not covered by the relevant legal provision (para. 37).
- For this reason, the Court held that the national provision does not constitute "prior information" within the meaning of Article 10, hence, the transfer does not comply with Article 10 of the directive (para. 38).
- The Court further examined whether Article 13 of the directive can be relied upon by the Member State to derogate from Article 10.
  - (1) The Court restated that the income data is not necessary to determine whether a person is insured.
  - (2) The definition of the data which can be transferred and the arrangements for transferring it are laid down in a Protocol established between the public bodies, which is not published officially (para. 40).
- The Court therefore concluded that the conditions laid down in Article 13 are not fulfilled (para. 41).

The processing does not comply with Article 11

- The Court further held that the CNAS, which did not obtain the data from the data subjects, must inform them of the identity of the data controller, the purposes of the processing and the categories of data processed in accordance with Article 11(1) (a) to (c) (para. 42).

- In light of the facts of the case, the Court found that the applicants did not receive such information (para. 44).
- The Court further stated that the national provision and the Protocol do not meet the requirements of Article 11(2) or those of Article 13 and the Member State cannot rely on this exception to derogate from Article 11(1) (para. 45).

Conclusion: "Articles 10, 11 and 13 of Directive 95/46/EC of the European Parliament and of the Council 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, must be interpreted as precluding national measures, such as those at issue in the main proceedings, which allow a public administrative body of a Member State to transfer personal data to another public administrative body and their subsequent processing" (Decision).

6) Case C-230/14, *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság*, 1 October 2015 - notion of establishment of the controller, applicable law, competent supervisory authority and power to impose penalties

Link

Facts of the case

Weltimmo, a company registered in Slovakia, runs a property dealing website regarding Hungarian properties. In this regard, it processes the personal data of the advertisers. The advertisements published on the website are free of charge for the first month while after a fee is to be paid. With the expiry of the first month, many advertisers asked the company to have their adverts deleted as well as their personal data. Irrespective of the request, Weltimmo not only did not proceed with the deletion, but also charged the advertisers for the prices of the services and forwarded their personal data to debt collection agencies.
The advertisers filed complaints before the Hungarian Data Protection Authority, which fined Weltimmo. The latter brought an action before the Administrative and Labour Court in Budapest and afterwards appealed the decision before the Supreme Court, which issued a preliminary ruling request to the EU Court of Justice on the interpretation of Article 4(1) and 28 (1), (3) and (6).

Main findings of the Court

Scope of application, notion of "establishment"

- The Court agrees with the opinion of the Advocate General in embracing a flexible rather than a formal definition of the "establishment". A data controller has an establishment, within the meaning of Directive 95/46 and particularly of Recital 19, **wherever there is an effective and real exercise of the activity through stable arrangements** (par. 29).
- Weltimmo developed two websites entirely written in Hungarian and regarding properties set in Hungary. Moreover, it did not carry out any activity at the place where it is formally registered and had changed the registered office from one State to another on several occasions. Lastly, the company opened a bank account in Hungary for recovering the debts, owned a letter box for everyday business affairs and has a formal representative in the same MS, who acted as an intermediary between the company itself and the advertisers; he also tried to negotiate the settlement of the

unpaid debts. It appears then that Weltimmo, although formally registered in Slovakia, is carrying out its activity in Hungary (par. 16 -18).

- In the light of the final goal pursued by the directive, which is effectively ensuring the protection of individuals personal data, even the presence of only one representative can, in some circumstances, suffice to represent stable arrangements if the same representative acts with a sufficient degree of stability. The company is therefore held to pursue a real and effective activity in Hungary. For this reason, since according to Article 4(1)(a) the MS shall apply the national provision adopted pursuant to the directive, Hungarian national law will be applicable to the case (par. 41).

Conclusion: Accordingly, Article 4(1)(a) of the Directive 95/46 must be interpreted as allowing the application of the DP provisions of a MS other than the MS in which the controller is registered, as long as it exercises a real and effective activity (also a minimal one) by means of stable arrangements (questions 1-6).

Power of the national supervisory authority to impose penalties

- The facts proving the real establishment of Weltimmo in Hungary are for the referring court to be verified (par. 33). The supervisory authority of a MS to which a complaint has been submitted in relation to the processing of his personal data shall examine it, irrespective of the applicable law. However, if the DP authority at issue reaches the conclusion that provisions other than the national ones are to be applied at the case since no establishment is found, the supervisory authority will not be endowed of the all powers conferred in accordance with the law of the MS. While on one hand the list of powers of article 28 (3) should not be considered as exhaustive and the powers of intervention may include the power to impose fines (par 49), on the other hand the mentioned powers of intervention must be exercised in compliance with the principles of territorial sovereignty and therefore not outside the jurisdiction of the Member State (par 59 - 60).
  On these grounds, the authority could not impose penalties on the basis of the law of another MS, but should, in accordance with article 28 (6) of the directive, conversely request the supervisory authority of that MS whose law is applicable to act in this regard (question 7).
- Accordingly, it shall, in fulfilment of **the duty of cooperation** laid down in Article 28(6) of the directive, request the supervisory authority of that other Member State to first establish an infringement of that law and then to impose penalties, based, where necessary, on the information which the authority of the first Member State has transmitted to the authority of that other Member State (par. 57).
- Lastly, the Court states that the Hungarian term used in the provision which transposed the directive into the Hungarian Law, meaning technical manipulation of data, shall be interpreted as having the same meaning as processing of data within the meaning of the directive (question 8).

7) C-362/14, *Maximillian Schrems v Data Protection Commissioner*, joined party Digital Rights Ireland Ltd, 6 October 2015 – Commission adequacy decision does not prevent a supervisory authority from examining a claim that a third country does not ensure an adequate level of protection + Commission Decision 2000/520 is invalid

Link

Facts of the case

Mr. Schrems lodged a complaint asking the Irish Data Protection Commissioner to prohibit Facebook Ireland from transferring his personal data to the United States. He submitted that the country did not ensure an adequate level of protection of personal data because of the surveillance activities conducted by the public authorities. The Commissioner considered that he was not required to investigate the complaint because of the lack of evidence and because the adequacy of data protection is determined by Decision 2000/520. Mr. Schrems challenged the Commissioner's decision before the Irish High Court which decided to ask the Court of Justice whether the Commissioner is bound by Community findings on the adequacy of protection in a third country or whether he can examine the claim of a person which contends that the level of protection is inadequate.

Main findings of the Court[2]

Powers of national supervisory authorities

- The Court recalled that Article 28 of the directive, Article 8(3) of the Charter and Article 16(2) TFEU require the Member States to establish "one or more public authorities responsible for monitoring, with complete independence, compliance with EU rules on the protection of individuals with regard to the processing of such data" (para. 40).
- The Court further noted that the national supervisory authorities' powers do not extend to personal data processed outside of their Member State but it specified that the transfer of personal data from a Member State to a third country constitutes 'processing of personal data' (paras. 44-45).
- Accordingly, the Court held that each national supervisory authority has "the power to check whether a transfer of personal data from its own Member State to a third country complies with the requirements laid down by Directive 95/46" (para. 47).
- The Court restated that Article 25 of the Directive makes clear that the finding that a third country ensures or not an adequate level of protection may be made by the Member States or by the Commission (para 50).
- Under Article 25(6) of the Directive, the Commission may adopt a decision stating that a third country ensures an adequate level of protection. This decision is binding on the Member States and all their organs (para. 51).
- For this reason, the Member States and their organs, including the national supervisory authorities, cannot adopt measures contrary to this decision until the decision is declared invalid by the Court (para 52).
- However, the Court stressed that such decision does not eliminate the powers of the national supervisory authorities with regard to the transfer of personal data to a third country subject of that decision (para. 54).
- It follows that the national supervisory authorities must be able to examine, with complete independence, whether the transfer of data complained of complies with the directive even if the Commission has adopted an adequacy decision (para. 57).
- The Court explained that a claim by an individual that the law and practices of a third country do not ensure an adequate level of protection, despite a Commission decision

[2] This summary builds upon a summary discussed within the International Transfers Subgroup of the Article 29 Working Party.

to the contrary, questions "whether the decision is compatible with the protection of the privacy and of the fundamental rights and freedoms of individuals" (para. 59).

- The Court recalled that it alone has the jurisdiction to review the compatibility of Union institutions acts, including Commission decisions (paras. 60-61).
- In a situation where the national supervisory authority comes to the conclusion that the arguments put forward in support of such a claim are unfounded and therefore rejects it, the person who lodged the claim must have access to judicial remedies enabling him to challenge such a decision adversely affecting him before the national courts. Those courts must stay proceedings and make a reference to the Court for a preliminary ruling on validity where they consider that one or more grounds for invalidity put forward by the parties or, as the case may be, raised by them of their own motion are well founded (para. 64).
- Where the national supervisory authority considers that the objections advanced by the person who has lodged a claim are well founded, **it must be able to engage in legal proceedings**, pursuant to the third indent of the first paragraph of Article 28 (3) of the Directive. It is incumbent upon the national legislature to provide for legal remedies enabling the national supervisory authority concerned to put forward the objections which it considers well founded before the national courts in order for them, if they share its doubts as to the validity of the Commission decision, to make a reference for a preliminary ruling for the purpose of examination of the decision's validity (para. 65).

<u>Conclusion:</u> *"(...) Article 25(6) of Directive 95/46, read in the light of Articles 7, 8 and 47 of the Charter, must be interpreted as meaning that a decision adopted pursuant to that provision, such as Decision 2000/520, by which the Commission finds that a third country ensures an adequate level of protection, does not prevent a supervisory authority of a Member State, within the meaning of Article 28 of that directive, from examining the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection" (para. 66).*

Validity of the Safe Harbour Decision

- In the view of the Court, the adequacy decision does not contain sufficient findings regarding the measure by which the United States ensures an adequate level of protection.
  According to Article 25(6) of Directive 95/46, the European Commission should consider the third country's level of protection as **essentially equivalent** to the one guaranteed in the EU legal order in order to issue an adequacy decision and should moreover give duly reasoned justification for this.
- Even though the directive 95/46 does not contain a specific definition of the notion of "adequate level of protection" it does refer to the need of conducting an assessment "in the light of all circumstances surrounding a data transfer operation". With this regard, the Court clarifies that the term "adequate", if it does not stand for an identical level of protection to be ensured, at least refers to an equivalent level of protection to the one ensured by the European Union by virtue of the Directive 95/46 read in the light of the Charter. In the view of the Grand Chambre, even though the recipient country has adopted means to ensure adequacy which may be different from the ones

used within the EU legal order, the same means must be practically ensuring an adequate, and then, equivalent level of protection as the EU does (par. 70-73).

- In this light, the European Commission is obliged to assess the content of all applicable rules resulting from domestic law or international commitments which are relevant for data transfer (par. 75).
- The Court clarifies that the European Commission is additionally in charge of periodically conducting checks on whether the finding may be still retained as factually and legally justified (par. 76).
- Notwithstanding the Court argues that there is no need for analysing the content of the SH principles, the Court takes the view that the reliability of a self - certification system essentially depends on the existence of an effective mechanism of both detection and supervision which would allow for any infringement to be detected and punished, this meeting the criterion of "adequacy". (par. 81)
- Firstly, SH principles are only applicable to self - certified US organizations receiving personal data from the European Union, not being binding for US public authorities as a consequence (par 82). Secondly, the adequacy assessed in the decision only refers to the provisions as implemented in accordance with the FAQs issued by the US Department of Commerce, without ever including findings related to the measure taken by the US to ensure the adequate and therefore equivalent level of the protection from a broader point of view (par. 83).
- Moreover, Annex I and IV, together combined, allow for interference in private life as long as reasons of national security and public interest require to do so: in this case, the lack of compliance with the SH principles will be justified on the grounds of the overriding legitimate interests established by US law, which must prevail on the same Safe Harbour principles, as to limit the mentioned interference with the fundamental rights or to any effective legal protection against interference of this kind (par. 85-87).
- Interference with private life is to be accompanied with a set of minimum safeguards, as established in the EU Charter. On the contrary, EC adequacy decision does not make any detailed reference to the safeguards which are taken by the US to ensure adequacy (par.91). Legislation which allows public authorities to access on a generalised basis the content of electronic communications must be considered as **compromising the essence of the fundamental right to respect for private life** as guaranteed by article 7 of the Charter.
- Similarly, legislation not granting effective legal remedies to access one's own personal data, to have data either rectified or erased, **compromises the essence of fundamental right to effective judicial protection** as guaranteed in article 47 of the Charter.

<u>Conclusion:</u> *Article 1 of the Decision 2000/520 is declared invalid since it does not comply with article 25(6), requiring for the third recipient country to ensure an adequate level of protection by reasons of its domestic law or international commitments.*

Excess of power from the Commission

- According to the Court, Article 28 of the directive, to be read in the light of Article 8 of the Charter, enables national supervisory authorities to examine, both with independence and due diligence, claims arising from individuals which may also raise questions on the compatibility of a EC adequacy findings with protection of fundamental rights law (par. 99).

- Article 3(1) of the adequacy decision makes the suspension of data flow to an organization having self - certified its adherence to the principles, possible only under restrictive conditions establishing a high threshold for intervention. In this sense, Article 3(1) must be read as hindering national supervisory authority from exercising the whole range of powers they are entitled to from article 28 of the directive 94/46 (par. 102) .

Conclusion: Article 3 of the Decision 2000/520 is declared as invalid for having the Commission exceeded the power conferred in Article 25(6) of the directive 95/46, depriving DPA from the power of diligently handling complaints in cases where compatibility of the EC adequacy decision is at issue.

"As Articles 1 and 3 of the Decision 2005/520 are inseparable from Articles 2 and 4 of that decision and the annexes thereto, their invalidity affects the validity of the decision in its entirety. (...) It is to be concluded that Decision 2000/520 is invalid (paras. 105-106)".

8) Case T-343/13, *CN v European Parliament*, 3 December 2015 - Petition to EP - Disclosure of personal data on EP's website

Link (not yet available in English)

Facts of the case

On 23 September 2009, CN, a retired former official of the Council, submitted a petition to the European Parliament ('EP') (via an on online form on the EP's website) with regard to EU support to disabled relatives of EU officials, career difficulties of EU officials coping with health problems, and the poor management of his case by the Council. The EP considered the petition admissible but rejected it.

Subsequently, the EP published on its website a "communication to the members" mentioning the applicant's name, his life-threatening disease and the severe disability of his son. In April 2012, the applicant asked for the deletion of this communication from the EP's website. Although the EP promptly replied - confirming the deletion of the communication -, the applicant held that such personal data were available on the EP's website until 10 January 2013. The EP maintains that the deletion of the data was complete as of 8 October 2012, and that the EP performed the deletion even if it was not legally obliged to do so.

The applicant, supported by EDPS, sought compensation for the material and non-material damage suffered as a result of the publication on the EP's website of the abovementioned data.

Main findings of the Court

- The EP's Communication regarding the applicant's petition disclosed personal data (the applicant's name and information on his career), health data (his life-threatening disease) and health data of a third party (the disability of his son) (para. 53).

On the disclosure of the applicant's data

- According to Article 10(1) of Regulation 45/2001, the processing of sensitive health data is prohibited, unless the data subject has given his express consent (Article 10(2)(a)). Therefore, the Court went on to assess whether this was the case or not (para. 56).
- In the process of lodging his petition, the applicant filled in a form agreeing to have it processed publicly and have his name listed in a public online register. The applicant could have instead chosen the confidential treatment of his petition (para. 65).
- The Court also noted that petitions are instruments of participatory democracy, conceived to stimulate the public debate on certain topics. In principle, petitions are public, unless petitioners ask to derogate to such a rule (para. 73).
- From the above, the Court maintained that the applicant gave a free, informed and express consent about the disclosure of his health data in accordance with Article 10(2)(a), and thus the EP behaved lawfully.
- With regard to the applicant's career data, Article 5(d) of Regulation 45/2001 states that personal data (other than sensitive data) may be processed only if the data subject has unambiguously given his consent.
- The same reasoning valid for health sensitive data should be applied *mutatis mutandis* to the applicant's career data. Also it is important to stress that the petition concerned specifically the neglecting by an EU body of the personal situation of the applicant in relation to his career (para. 79).
- Therefore, the Court held that the applicant expressed a free, specific and informed indication of his will with regard to the processing of his data as part of the treatment of the petition by the EP, in line with Article 5(d) (para. 80).

On the disclosure of the applicant's son data

- With regard to the EP disclosure of data regarding the applicant's son and his disability, the Court held that the applicant's expressed consent cannot refer to health data of his son, in the absence of proof of legal custody (para. 84).
- However, the Court held that one only can plead infringement of the rights of a subject to which a norm confers such rights. In the present case, the applicant's son is not part of the recourse and there is no proof of the applicant's legal custody. Consequently the applicant cannot claim violation of his son's rights (para. 86).

On the request of deletion of the data from the EP's website

- The Court went on to assess whether the applicant had the right to request the deletion of his data by the EP (para. 89).
- According to Article 16 of Regulation 45/2001, the data subject can request the erasure of his data to the controller if their processing is unlawful, which was not the case here (as noted above). Furthermore, Article 18 states that the data subject can object to the processing of his data, unless he unambiguously gave his consent to it (Article 5(d)), which was the case here (as previously said) (para. 90 and 91).
- Also, since the processing of the applicant's data is based on his consent, the Court noted that the withdrawal of consent is not provided for by Regulation 45/2001 (para. 92).
- The Court therefore held that the applicant could not legitimately claim the right of erasure of his data by the EP on the basis of Regulation 45/2001 (para. 93).

- If, on one side, the right to private life includes the right of the individual not to disclose details of his health conditions, on the other hand the judgments quoted by the applicant to support the defence are not based on the circumstance of the present case, that is, the consent given by the data subject (paras 102 -106).
- Accordingly, whenever the data subject gives consent to the disclosure, intrusion into private life by public authorities and an infringement of article 8 ECHR do not occur (paras 107-108).

9) C-419/14, *WebMindLicenses Kft. v. Nemzeti Adó-és Vámhivatal Kiemelt Adó-és Vám Foigazgatóság*, 17 December 2015 - value added tax, abuse of rights, right to defence, Directive 206/112/EC and interception of telecommunications

Link

Facts of the case

WebMindLicenses ('WML') is a company registered in Hungary that acquired free of charge from Hypodest Patent Development Company (in Portugal) a know-how enabling a website to be operated through which erotic interactive audio-visual services in which individuals throughout the world took part in real time were supplied. On the same day, WML made that know-how available by a licensing agreement to Lalib, also established in Portugal.

Following a tax inspection, the Hungarian tax authorities required WML to pay the Hungarian VAT, a fine and penalties for late payments, alleging that the transfer of that know-how was not a genuine economic transaction since the know-how was in reality exploited by WML, but a way of circumventing Hungarian tax law, which was less advantageous than Portuguese Law.

WML brought an action against the National Tax and Customs Authority on the ground that it had used evidence by means of intercepting telecommunications and seizing emails in the course of a parallel criminal procedure.

The Hungarian Administrative and Labour Court referred a preliminary ruling made up of 17 questions, of which questions10 to 15 are relevant for data protection and were examined by the Court of Justice altogether. The Hungarian Court was notably uncertain *"whether it is to be inferred from the objectives of the VAT Directive that the tax authorities may gather evidence obtained in the context of a criminal procedure, including by secret means, and use it as the basis for an administrative decision. In this connection, (...) it raises the question of* ***what limits the Charter places on the institutional and procedural autonomy of the Member States****"*.

Main findings of the Court

- The Court took the view that the national rules of evidence should be used to assess whether an action constitutes an abusive practice. However, those rules cannot undermine the effectiveness of EU law. (par. 65)
- According to settled case-law, fundamental rights are applicable to all situations governed by EU Law. In this case the Court considered that the VAT adjustment at issue constitutes an implementation of EU law for the purposes of article 51(1) of the Charter. Furthermore, the Court found that *"EU Law does not preclude the tax authorities from being able in the*

*context of an administrative procedure (...) to use evidence obtained in the context of a parallel criminal procedure that has not yet been concluded, **provided that the rights guaranteed by EU law, especially by the Charter, are observed**"*. (par. 66-68)

- The interception of telecommunications and the seizing of emails constitute an interference with the right laid down in Article 7 of the Charter. Therefore limitations must comply with the conditions set out in Article 52(1). (par. 71-73)

1) As regards the principle of proportionality, the Court reminded that the measures adopted by Member States must not go further than necessary to meet the objective of general interest being pursued. (par. 74)
2) The VAT Directive aims *inter alia* at preventing possible tax evasion, avoidance and abuse. Therefore, investigative measures carried out with a view to prosecuting offences in that sphere meet an objective of general interest recognised by the European Union. (par. 76)
3) As for the necessity of the investigative measures, knowing that the emails were seized without judicial authorisation, the Court reminded that *"in the absence of prior judicial authorisation, **a strict legal framework** for, and **strict limits** on, such seizure are required if individuals are to be protected from arbitrary interference by the authorities with the rights guaranteed under Article 7 of the Charter. (...) It is incumbent upon the referring court to examine (...) the availability to the person concerned by the seizure of an **ex post factum judicial review** relating to both the legality and necessity of the seizure."* (par. 77-78)

- On one hand, the Court found that there was no need to assess if the gathering and use of that evidence by the tax authorities interfered with the right to protection of personal data enshrined in Article 8 of the Charter, since WML is not a natural person (par. 79). On the other hand, the use of that evidence constitutes as such a limitation on the exercise of the right guaranteed by Article 7 of the Charter. It must therefore be examined whether that use satisfies as well the requirements set out in Article 52(1). (par. 80)
- When considering the necessity for such use, it must be assessed whether the same information could not have been obtained with less privacy-intrusive means than the interception of telecommunications and seizure of emails, such as an inspection at WML's premises and a request for information or for an administrative enquiry sent to the Portuguese authorities. (par. 82)
- The Court concluded that *"it is incumbent upon the national court which reviews the legality of the decision founded on such evidence adjusting VAT to verify, first, whether the **interception** of telecommunications and seizure of emails were means of investigation provided for by law and were necessary in the context of the criminal procedure and, secondly, whether the **use** by the tax authorities of the evidence obtained by those means was also authorised by law and necessary. (...) If the national court finds that (...) that evidence was obtained in the context of the criminal procedure, or used in the context of the administrative procedure, in breach of Article 7 of the Charter, it must disregard that evidence and annul that decision if, as a result, the latter has no basis. That evidence must also be disregarded if the national court is not empowered to check that it was obtained in the context of the criminal procedure in accordance with EU law or cannot at least satisfy itself, on the basis of a review already carried out by a criminal court in an inter partes procedure, that it was obtained in accordance with EU law."*

ACCESS TO DOCUMENTS

1) T-341/12, *Degussa*, 28 January 2015 - whether the disclosure of information in the context of infringement proceedings in the field of competition law is protected by Article 8 ECHR

Link

Facts of the case

The applicant, Evonik Degussa GmbH, is a company active in the hydrogen peroxide and perborate sector which had participated in an infringement of competition law with 16 other companies. As the applicant had fully cooperated and provided the Commission with all the information in its possession concerning the infringement, it was granted complete immunity from fines.

After adopting an infringement decision, the Commission informed the applicant of its intention to publish a more complete non-confidential version of the Decision on the DG COMP website. The applicant objected to this publication contending that it included confidential information, but this was rejected by the Commission and also later by the hearing officer to whom the matter was referred.

The applicant brought proceedings to annul the decision of the hearing officer on various grounds, notably a breach of its right to protection of its private life, as guaranteed in Article 8(1) of the ECHR and now enshrined in Article 7 of the Charter of Fundamental Rights.

Main findings of the Court

Alleged breach of the right to protection of private life (paras 123-127)

- In Commission v Editions Odile Jacob, the Commission acknowledged that *"information submitted by undertakings which are parties to a merger must be regarded as relating to their private activity and as such are subject to compliance with the provisions of Article 8 of the ECHR"* (para 124).

- However, the Court recalled that a person cannot rely on this article *"to complain of a loss of reputation which is the foreseeable consequence of his own actions, such as the commission of a criminal offence"* (para 125).

Conclusion: The Court found that the right to protection of private life enshrined in Article 8 ECHR does not prevent the disclosure of information concerning *"an undertaking's participation in an infringement of EU law relating to cartels"* (para 126).

2) T-188/12, Breyer, 27 February 2015 - Access to documents - inclusion of written submissions lodged by Member States within the scope of the right of access to documents

Link

Facts of the case

The applicant introduced a first application for access to all documents related to infringement proceedings brought by the Commission against Germany and Austria concerning the transposition of the e-privacy Directive. This application was rejected and the applicant submitted a confirmatory application. The Commission granted access to some of the documents but refused access to the written submissions submitted by Austria in the proceedings on the ground that they are not covered by Regulation 1049/2001.

The applicant brought proceedings for annulment of the decision in so far at it denies access to Austria's written submissions.

Main findings of the Court

1) The classification of the written submissions as documents held by an institution within the meaning of Article 2(3) of Regulation 1049/2001 in conjunction with Article 3(a)

- The Court recalled that Regulation 1049/2001 *"is intended (...) to give the fullest possible effect to the right of public access to documents of the institutions"* (para 39).
- Under Article 2(3) of Regulation 1049/2001, it applies to *"all documents held by an institution, that is to say drawn up or received by it and in its possession, in all areas of European Union activity"*. Article 3(b) expressly refers to documents received from the Member States (para 40).
- The term 'document' is defined broadly as long as it relates to the policies, activities or decisions of an institution (paras 41-42).
- In light of the broad definition, and the fact that Article 4(2) only prevents access to documents relating to court proceedings where disclosure would undermine the proceedings, the Court found that Regulation 1049/2001 did not intend on excluding the "institutions' litigious activities" from the right of access (para 43).
- The Commission brought an action against Austria, the Court sent to it copies of the written submissions and the copies have been in the possession of the Commission (paras 44-46).
- It follows that *"the Commission, in the exercise of its powers in respect of its litigious activities, received documents drawn up by a Member State, which is a third party within the meaning of Article 3(b) of Regulation 1049/2001, and that those documents are in its possession within the meaning of Article 2(3) of that regulation in conjunction with Article 3(a) thereof"* (para 47). Therefore, the written submissions constitute documents held by an institution within the meaning of Regulation 1049/2001. (para 48).
- In response to the Commission's arguments, the Court added that the documents do not need to have been addressed to the Commission or sent directly by the Member States and it stressed that it is irrelevant whether the documents are copies or originals (paras 50-54).
- Furthermore, the Court rejected the claim that Regulation 1049/2001 only covers administrative activities and confirmed that the Commission received the submissions in the exercise of its powers, i.e. its power to bring an action against a Member State for failure to fulfil an obligation under Article 258 TFEU (paras 55-62).

2) The effect of the fourth subparagraph of Article 15(3) TFEU on the application of Regulation 1049/2001

- First, the Court stated that judicial activities are excluded from the scope of the right of access to documents and that the principle of transparency only applies to the Court of Justice with regard to its administrative tasks pursuant to Article 15(3) TFEU (paras 67-69).
- Moreover, the Court has already held that Commission's written submissions *"are inherently more a part of the judicial activities of [the EU Courts] than of the administrative activities of the Commission"* (para 70). This finding also applies to a Member State's written submissions (para 72).
- In light of the case-law, the Court pointed out that the Commission's written submissions fall within Regulation 1049/2001 despite the fact that they form part of the judicial activities of the EU Courts which are excluded from the right of access to documents pursuant to Article 15(3) (para 74). Their inclusion within the scope of the Regulation is supported by the fact that the Court has previously ruled that such submissions fell within the scope of the exception to the principle of transparency under Article 4(2) where disclosure would undermine the protection of court proceedings (paras 75-78).
- To the extent that written submissions lodged by an institution are not excluded from the right of access by virtue of Article 15(3), submissions lodged by a Member States should not be excluded either (paras 79-80).
- In response to the Commission's arguments, the Court confirmed there is no authorship rule, which would require distinguishing between submissions lodged by an institution and those lodged by a Member State (para 81).
- Instead, a distinction should be drawn between the judicial activities excluded from the scope of the right of access documents pursuant to Article 15(3) TFEU and written submissions, which are part of the judicial activities but are not excluded (para 82). As a result, they fall within the scope of Regulation 1049/2001 if the conditions of its application are fulfilled and none of the exceptions apply, including "the possibility under Article 4(5) for the Member State to request the institution concerned not to disclose its written submissions" (para 83).

Conclusion: The application for annulment is granted (para 114):

- Written submissions lodged by a Member State constitute documents held by an institution within the meaning of Regulation 1049/2001 (para 48).
- The fourth subparagraph of Article 15(3) does not preclude the inclusion of the written submissions within the scope of Regulation 1049/2001 (para 83).

3) T-480/11 *Technion - Israel Institute of Technology, Technion Research & Development Foundation Ltd v. European Commission*, 12 May 2015 - Access to Documents - exception for the protection of inspections, investigations and audits, obligation to carry out a specific and individual examination, overriding public interest.

Link

Facts of the case

In 2003 Technion, a higher education institution in the field of technology, concluded four contracts with the Commission of the European Union within the sixth framework

Programme of the European Commission for research, technological development and demonstration activities. The Commission decided in 2009 to carry out a financial audit on the costs claimed in the context of three of the four contracts, following to which the auditor proposed some adjustments mainly concerning staff costs. In particular, the auditor observed that Mr K. was working for several bodies during the audited period, although he had been hired to work full time at Technion, and that was, to this respect, impossible to assess time and costs claimed for his performed services. In 2010 the Commission granted the request from Technion of an extension period for submitting comments, yet it claimed that it could not provide copies of administrative and financial documents of the financial audit as they were carried out on a confidential basis. Technion challenged the refusal contending that no exception in Regulation 1049/2001 could justify it. In relation to this, the Commission replied that the documents were totally covered by the exception provided in Article 4(1)(b) of Regulation 1049/2001, relating to the protection of the purposes of inspections, investigations and audits.

Technion submitted a confirmatory application to the Secretary-General of the Commission for access to the documents. The latter, by confirming the refusal, claimed that it was impossible to describe the documents without disclosing their contents, that the documents requested, as they contain personal data on Mr. K and other people could not be disclosed since they were covered by the exception under Article 4(1)(b) of Regulation 1049/01, and lastly that Technion had failed to prove the existence of a public interest able to override the damage caused by the disclosure.

The court analysed in conjunction the first three pleas in law: the applicant alleged that the Commission failed in carrying out a specific and individual examination of the documents, had incurred in a manifest error of assessment in the application of the exceptions under Regulation 1049/2001 and had the infringed Article 4(6) as its refusal to grant partial access to documents.

With the fourth plea in law, the applicant alleged an infringement of the principle of proportionality resulting from failure to weigh the exception against the public interest.

Main findings of the Court

- The Court found that exceptions to access to documents had to be constructed and applied strictly so to no undermine the general principle of giving the public the widest possible access to EU institutions documents (par 43).
- However, the mere fact that a document relates to an interest protected by an exception cannot justify the application of the exception *per se*, as the Institution has the obligation to previously assess whether the access might undermine the protected interest and whether there is no a public overriding interest in the disclosure (par. 44) The institution, moreover, has to carry out the examination in respect of each document (par. 44-46).
- Nevertheless, there are exceptions to the obligation of carrying out a concrete and individual examination of the documents. Such an examination may not be necessary where, due to particular circumstances of the case, it is obvious that access must be refused, or on the contrary, granted. (par. 48).
- In the view of the Court, the access would have undermined the protected interests severely: as the audit was still in progress at the time it was contested, access might increase the foreseeable risk that the disclosure could, in particular, expose the auditor to outside pressures, with the potential effect of undermining the effectiveness of Technion

audit. The disclosure might also restrict the Commission freedom to carry out audits and further investigations on the basis of the findings of Technion audit (par. 57). Moreover, under the General Conditions appearing in Annex II to the contracts, the audit undertaken by the Commission had to be carried out on a confidential basis. Therefore, the disclosure of the documents would undermine the very existence of the clause of the contract. (par. 58)

- Following the previous considerations, the Commission was entitled to take the view, without being necessary to carry out a specific and individual examination of each of the documents, that access was to be refused on the basis of Article 4(2) of Regulation 1049/01. (par. 59)
- Also, the Commission was equally justified in holding that the documents were covered in their entirety by the exception, so that no partial access could have been granted (par. 60).
- In the view of the Court, as the purpose of Regulation 1049/2001 is to guarantee access for everyone to public documents and not merely access for the requesting party do documents relating to him (par. 74), the individual interest cannot be taken into account for the assessment of an overriding public interest (par. 75).
- Therefore, the alleged interest of other bodies which participated in the projects concerned at the disclosure of the documents as to determine whether the audits were lawful, has to be defined as a private interest (par. 77). Given also that in the present case, the interest of the public in transparency was not pressing, it could not outweigh the interest in protecting the purposes of inspections, investigations and audits. Accordingly, the interest in the transparency of audits, does not amount to an overriding public interest within the meaning of Article 4(2) of Regulation 1049/2001. (par. 83)
- The Court found that the application of the exceptions were not marred by any error and that **any possible errors of law or assessment committed by the Commission relating to the protection of privacy and the integrity of individual would have no effect on the legality of the present decision**. (par. 85)

4) T-496/13, *Colin Boyd McCullough v Cedefop*, 11 June 2015 - Access to documents, exception relating to the protection of privacy and integrity of individual

Link

Facts of the case

In 2013, Mr McCullough, a former employee of the European Centre for Development of Vocational Training ('Cedefop'), requested access to the minutes of all meetings of its Governing Board on the basis of Regulation 1049/2001 in order for him to prepare his defence against Cedefop in legal proceedings in front of the Greek Courts.

Cedefop rejected Mr McCullough's access request (*inter alia*) on the basis of the exception concerning the risk that privacy and the integrity of the individual would be undermined, provided for in Article 4(1)(b) of Regulation 1049/2001. Cedefop considered that the names of the members of its Governing Board and its Bureau, which were contained in those minutes, constituted personal data protected by that provision and by Regulation 45/2001, and that access to those documents by a third party could lead to a serious violation of the privacy and the integrity of the members, as their opinions and their views on the matters discussed would be clearly shown by those documents.

Mr McCullough asked for the annulment of the Cedefop's refusal decision alleging notably that EU law had been infringed by a misinterpretation of Article 4(1)(b) of Regulation 1049/2001.

Main findings of the Court

- In its preliminary considerations, the Court observed that Regulation 1049/01 aims at giving the fullest possible effect to the right of public access to documents of the institutions, subject to certain limitations based on grounds of public or private interest laid down in Article 4 of the same Regulation. The Court reminded that those **exceptions must be interpreted strictly**. Regulation 1049/2001 and Regulation 45/2001 pursue different objectives. Since they do not contain any provisions granting one regulation primacy over the other, in principle, their full application should be ensured. The Court further described Article 4(1)(b) of Regulation 1049/01 as an **indivisible provision**, requiring that any undermining of privacy and integrity of individuals be examined in conformity with EU legislation concerning the protection of personal data. In accordance with the case-law, when a request based on Regulation 1049/2001 seeks to obtain access to documents including personal data, the provisions of Regulation 45/01 become applicable in their entirety. (par 36-44)

On the existence of personal data and the application of Regulation 45/2001

- The Court reiterated that **surnames are personal data** and thus are protected by the provisions of Regulation 45/2001. *"The fact that the members of Cedefop's decision-making bodies participated in the meetings of those bodies in connection with the exercise of their public duties and not in the private sphere, or the fact that the surnames of the members of the Governing Board and the Bureau were published in the Official Journal of the European Union or on the Internet, does not affect the characterisation of their surnames as personal data."*(par. 66)

- Therefore, the surnames of the Governing Board and the Bureau may be transferred to a third party only in case that transfer meets the conditions of Article 8(a) or (b) of Regulation 1049/2001. In this regard, it is for the person requesting access to establish the necessity of transferring the requested data, the proof of which, according to the Court, Mr McCullough has failed to provide to Cedefop. (par. 67-70) Accordingly, Cedefop was fully entitled to refuse the transfer of personal data. (par. 79)

On the absence of any risk that the protection of the privacy would be undermined by the disclosure

- Nonetheless, the analysis made by Cedefop in relation to the access request is found by the Court to be incomplete, having failed to carry out an examination demonstrating that granting access to those documents would specifically and actually undermine the privacy of those members, nor verified whether the risk of the protected interest being undermined was reasonably foreseeable and not purely hypothetical.
    - First, it is not apparent how the decision and views expressed in these meetings fall within the sphere of privacy, as they were professional meetings.
    - Secondly, the access request covers a considerable number of documents drawn up over four years but the refusal decision at issue does not contain any

assessment of how their disclosure might specifically and actually undermine the protection of privacy.

It must be inferred from such a finding that Cedefop has not proved that the requested documents fall within the exception of Article 4(1)(b). (par. 86-88)

- In addition, the Court acknowledged that it is open to the institution concerned to base its decision on general presumptions as considerations of a similar kind likely to apply to access requests relating to documents of the same nature. However, Cedefop at no point demonstrated that the various documents requested were part of the same category of documents, which may have justified the generic decision. In addition, it appears very unlikely that the subjects addressed over four years relate to the same individual procedure or area. (90-92)

Conclusion: The Court annulled the refusal decision of Cedefop of 15 July 2013 in so far as that decision refuses access to the minutes of the Governing Board and the Bureau, except as regards access to the surnames of the members of the Governing Board and the Bureau.

5) T-214/13, *Typke*, 2 July 2015 - Access to documents is not a general right to access data - whether data stored in various databases constitutes an existing document

Link

Facts of the case

The applicant is a member of the staff of the European Commission who participated in an EPSO competition. After the publication of the results, he requested access to a table containing a set of anonymised data on the admissions tests. EPSO refused his request on the ground that, while the information was indeed stored in several databases, the table did not exist. As a result, the applicant filed a confirmatory application with the Secretariat General specifying that his request did not require a new document to be created and that providing the several relevant documents would suffice. The Secretariat-General rejected the confirmatory application on the grounds that it requested a document which did not exist. Moreover, even if the application could be understood as requesting access to separate documents, this would be disproportionate in light of the workload that it would require.

The applicant brought proceedings to annul the refusal decision.[3] He contests the Secretariat-General's finding that his application does not concern an 'existing document' within the meaning of Regulation 1049/2001 (para 41).

Main findings of the Court

[3] Please note that the applicant actually brought proceedings against two confirmatory decisions. The second decision consisted of the absence of a response in due time by the Secretariat-General relating to another confirmatory application. The applicant had filed this application in the context of a second request for access to the same documents initiated in reaction to the absence of response by the Secretariat-General with regard to the first confirmatory application. However, the Secretariat-General issued an explicit confirmatory decision during the course of the proceedings, which brought this implied decision outside the scope of the proceedings.

- The Court first pointed out that the excessive burden of work required by an application, even if it affects the proper functioning of the administration, is irrelevant in assessing whether the request is admissible (paras 50-51).
- Although the term 'document' is given a broad definition, it must be distinguished from the concept of information (para 53), i.e. *"a data element that may appear in one or more documents"* (para 54). In that regard, the Court held that, although the Regulation grants the public a right of access to a Commission document, the Commission is not obliged *"to reply to any request for information from an individual"* (para 54).
- In its previous case-law, the Court established that the right of access under Article 2(3) of the Regulation is limited to existing documents. Requesting a new document, even it is based on information found in existing documents, cannot be considered as an application for partial access (para 55).
- However, if the application requests the Commission to carry out a search in existing databases, the Commission is obliged to accede to the request, subject to the exceptions under Article 4 of the Regulation, *"if the requisite search can be carried out using the search tools which it has available for the database in question"* (para 56). As a result, *"anything that can be extracted from them by means of a normal or routine search may be the subject of an application for access"* (para 59).
- In the present case, the raw data relating to the admission tests is indeed in the possession of the Commission (para 60). However, the Court found that the applicant did not request access to the database or part of it. Instead, he requested a set of information relating to the tests *"selected in accordance with criteria and in a format specified by"* him (para 61).
- The Court held that the *"selection of the information sought by the applicant thus involves a number of separate operations, including certain data processing operations in respect of the data concerned"* (para 62).
- The Commission stated that it does not have the required search tools. The Court recalled that a presumption of legality applies to statements of the institutions regarding the non-existence of documents and it applied this presumption to statements relating to the combination of data (paras 65-66).
- In light of the facts, the Court found that *"the operations involved in that programming work (...) are not comparable to a normal or routine search"* because it would require developing new search tools (para 68). Moreover, neither the existing individual statements sent to the candidates nor the matrix described in the EPSO's call for tenders support the argument that the application relates to one or more existing documents (paras 71-79).

Conclusion: *"the application (...) does not relate to access, even partial, to one or more existing documents held by EPSO, but, on the contrary, relates to the production of new documents which cannot be extracted from a database by means of a normal or routine search using an existing search tool."* (para 80)

6) T-115/13, *Dennekamp v Parliament,* 15 July 2015 – access to documents relating to the affiliation of MEPs to the additional pension scheme

Link

Facts of the case

Mr Dennekamp is a journalist who first requested access to documents relating to the affiliation of certain MEPs to the additional pension scheme on the basis of Regulation 1049/2001 in November 2005. His first application to the Court in Case T-82/09 was dismissed in December 2008 on the basis that he had failed to comply with the requirement to show necessity for the transfer under Article 8(b) of Regulation 45/2001, following the ruling by the Court of Justice in Case C-28/08 P, Bavarian Lager in June 2010.

In his second initial application in September 2012, he submitted that there was an objective necessity within the meaning of Article 8(b) of Regulation 45/2001 for the personal data to be transferred relying on the existence of a broad public interest in transparency. Furthermore, he argued that there was no risk that the data subjects' legitimate interests would be prejudiced by disclosure of the data concerned because it would not affect their private interests. The application was refused on the ground that the applicant failed to demonstrate the necessity for the data to be transferred by referring exclusively to the public interest in transparency.

In his confirmatory application, Mr Dennekamp applied again for access to the documents relying on the right of access to information and the right to freedom of expression. The European Parliament rejected the application on the basis of the exception relating to a risk for the privacy and the integrity of the individual being undermined, as provided for in Article 4(1)(b) of the Regulation 1049/2011, on the grounds that those documents contained personal data within the meaning of Article 2(a) of Regulation 45/2001, disclosure of which would be contrary to that regulation, which must be applied in its entirety where the documents requested contain such data.

The applicant sought to annul the EP decision rejecting his confirmatory application.

The EDPS supported the applicant in this case, as well as in the earlier Case T-82/09. The EDPS noted in particular that personal data of MEPs were being processed within their public rather than their private sphere and that there was no reason to expect that a transfer of the requested information would prejudice this lower standard of legitimate interest.

Main findings of the Court

- The Court first noted that the names of 65 MEPs who were members of the additional pension scheme had been made public in previous rulings given by the Court and were therefore outside of the scope of the ruling (paras. 25-29).

Infringement of Articles 11 and 42 of the Charter and error of law in application of Article 4(1)(b) of Regulation 1049/2001 read in conjunction with Article 8(b) of Regulation 45/2011

Legislative framework

- The Court stated that if an application for access to documents may result in the disclosure of personal data, the institution must apply all the provisions of Regulation 45/2001, and the full scope of the protection afforded to those data may not be limited as a result of the various rules and principles in Regulation 1049/2001 (para. 51).
- Article 8(b) of Regulation 45/2001 requires the institution to assess the necessity and proportionality of the request in light of the applicant's objective. Furthermore, the institution must examine whether the legitimate interests of the data subjects might be

prejudiced by granting the request in light of the applicant's objective. For this reason, the institution must assess the justification for access to the documents given by the applicant (para. 54).

- Although this observation amounts to the recognition of an exception to Article 6(1) of Regulation 1049/2001, the Court ruled that is justified by the *effet utile* to be given to the provisions of Regulation 45/2001, in particular Article 8(b) (para. 55).
- The Court stressed that the **conditions to transfer personal data must be interpreted strictly**. The condition of necessity is fulfilled where the applicant gives express and legitimate reasons showing that the transfer of personal data is the most appropriate of the possible measures for attaining the applicant's objective, and that it is proportionate to that objective (para. 59).
- The Court argued that this strict interpretation would not prevent any access to documents because it does not follow that a general justification, such as the public's right to information concerning the conduct of MEPs, cannot be taken into consideration (paras. 60-61).
- The Court summarized its findings as follows (para. 68):
    - the condition of necessity laid down in Article 8(b) of Regulation 45/2001 must be strictly interpreted;
    - it requires an examination in light of the objective pursued by the applicant, thereby restricting the scope of the rule on the absence of justification for an application for access;
    - the justification may be of a general nature (so long as it makes it possible to determine whether the transfer of data is the most appropriate of possible measures – see below);
    - Regulation 1049/2001 must not be rendered devoid of purpose by an interpretation of the relevant provisions that would mean that legitimate disclosure could never have the aim of full disclosure to the public.

Application to the facts of the case

- In the contested decision, the EP found that the public interest in the expenditure of public money, including the financial benefits enjoyed by MEPs, was abstract and very general. Moreover, the EP asserted that the applicant failed to prove the necessity to receive the specific personal data requested to achieve his aim because the Bureau, and not all members of the schemes, was in charge of making decisions with regard to the additional pension scheme and because he failed to identify a particular and specific risk of conflict of interest (para. 73).

**Right to information and right to freedom of expression*

- The Court held that relying on the right to information and the right to freedom of expression **is not sufficient** to establish that the transfer of the names of the MEPs participating in the additional pension scheme is the most appropriate of the possible measures to inform the public and enable it to take part in a debate on the legitimacy of the scheme or that it is proportionate to it (paras. 81 and 87). **For this reason, Articles 11 and 42 of the Charter have not been infringed** (para. 87).

The applicant merely asserted (...) that the measures designed to provide public control over public expenditure in the context of the additional pension scheme (...) did not protect the fundamental rights he had invoked (...) and that those measures could not, therefore, justify the non-disclosure of the data at issue. It must be noted that ***it cannot be determined from those points in what respect the transfer of the names of MEPs participating in the scheme is the most appropriate measure for attaining the applicant's objective, or how it is proportionate to that objective****. The mere assertion that that transfer would best ensure the protection of fundamental rights cannot be considered to have been the result of even a limited analysis of the effects and implications of the various measures that might be adopted in order to meet the applicant's objectives.* (para. 83)

** Bringing to light the possible conflicts of interests of MEPs*

- The applicant also argued that access to the documents is necessary to determine whether MEPs' voting behaviour with regard to the additional pension scheme is influenced by their financial interests and the Court identified the objective of the applicant as the bringing to light of possible conflicts of interests of MEPs (paras. 88-89). It described this conflict as the possibility for MEPs to amend the additional pension scheme or express their views on it in such a way as to promote their interests as beneficiaries of the scheme (para. 93).

a) Necessity

- The Court held that the transfer of the names is the most appropriate measure to determine whether the interests that MEPs have in the scheme can influence their voting behaviour and it is proportionate to it (para. 94). However, the disclosure of the names is not sufficient to reach this objective and it is also necessary to know which MEPs voted on the scheme (para. 95).
- The Court noted that it is sufficient to demonstrate the existence of a possible conflict of interest: *'For the purpose of bringing to light the potential conflicts of interests of MEPs voting on the additional pension scheme, the applicant was, as a matter of law, entitled merely to show that they were in that situation because of their dual role as MEPs and as members of the scheme.* ***The concept of a conflict of interest*** *relates to a situation in which the interest identified may, in the eyes of the public, appear to influence the impartial and objective performance of official duties and does not, therefore, require the lack of any impartial performance of the duties in question to be demonstrated' (para. 110).*
- The Court found that the EP made a manifest error of assessment when it found that the applicant had not established the necessity to transfer the names of the MEPs who had voted on the scheme in light of the aim of bringing to light potential conflicts of interests (para. 113).

b) Prejudice to the legitimate interests of the data subjects ***(personal data falling within the public or the private sphere of the MEPs)***

- The Court recalled that an EU institution which receives a request of access to documents including personal data must refuse if there is the slightest reason to assume that the data subjects' legitimate interests would be prejudiced (para. 117).

- The Court noted that it must be taken into account that public figures have generally already accepted that some of their personal data will be disclosed to the public (para. 119). For this reason, it is necessary to identify whether the personal data requested falls within the public or private sphere of the MEPs. In that regard, the Court found that **the personal data concerned falls within the public sphere of the MEPs** because it is necessary to be an MEP in order to join the additional pension scheme and because of the significant financial and legal commitment of the Parliament to the scheme (paras. 120-121).
- The legitimate interests of the MEPs must therefore be subject to a lesser degree of protection than the one that would be afforded to interests falling within the private sphere (para. 124).
- The Court further held that the legitimate interests of the MEPs who are members of the additional pension scheme cannot be prejudiced by the transfer of the personal data at issue in view of the importance of the interests invoked which are intended to ensure the proper functioning of the European Union by increasing the confidence that citizens may legitimately place in the institutions (para. 126).
- The Court warned against the incorrect assertion of the EP that there is a legally binding presumption favouring the legitimate interests of the data subjects (para. 127).
- The Court declared that the EP made a manifest error of assessment in finding that the legitimate interests of MEPs participating in the additional pension scheme who took part in a vote on it might be prejudiced by the transfer of their names (para. 130).
- However, the Court specified that this finding **is limited to those members who took part in the votes** on the pension scheme (para. 131).

Failure to state reasons

- The Court explained that the institution must, in principle, explain how disclosure could specifically and actually undermine the protected interests (para. 133).
- In this case, the Court held that despite the relatively succinct reasoning of the EP in the contested decision, the EP did not fail to state reasons (para. 141).

Conclusion:

"(...) 2. Annuls Decision A(2012) 13180 in so far as access is thereby refused to the names of Members participating in the additional pension scheme of the European Parliament who, as members of the Parliament's plenary, actually took part in the votes on that additional pension scheme held on 24 April 2007, 22 April 2008 and 10 May 2012"

7) Case C-615/13, *ClientEarth and Pesticide Action Network Europe (PAN Europe) v European Food Safety Authority (EFSA)*, 16 July 2015 - right to access to documents of EU institutions, concept of personal data, conditions for transfer of personal data

Link

Facts of the case

The European Food Safety Authority ('EFSA') established on 25 September 2009 a working group entrusted with the development of a guidance document on how to implement Article

8(5) of the Regulation No 1107/2009 concerning the placing of plant protection products on the market.

The working group submitted a draft to two EFSA bodies (i.e. the Plant Protection Products and their Residues Panel and the Pesticide Steering Committee), whose members were external experts, and incorporated their comments in the draft. The Working Group then subjected the document to a public consultation, with also PAN Europe involved.

In November 2010, ClientEarth and PAN Europe jointly submitted to EFSA an application requesting access to the sets of documents relating to the preparation of the draft guidance document. On 1 December 2010, EFSA granted a partial access to these documents and, following the request made by the applicants to reconsider that position, by decision of 10 February 2011, EFSA confirmed that access to the documents was refused under the second subparagraph of Article 4(3) of Regulation 1049/2001.

In April 2011, ClientEarth and PAN Europe brought an action for the annulment of the first decision, later extended also to the second one. The General Court dismissed the action holding that the pleas were unfounded. ClientEarth and PAN Europe finally appealed against the General Court decision.

With the first ground of appeal, ClientEarth and PAN Europe criticise the finding of the General Court, claiming a misapplication of the concept of "personal data" within the meaning of Article 2(a) of Regulation No 45/2001: in their view, an expert issuing a scientific opinion, in a professional capacity, is not covered by the concept of privacy (par. 23-25).

By the second and third grounds of appeal, the appellants maintain that neither the General Court nor EFSA weighted the conflicting rights to transparency and to protection of privacy and personal data (par. 38) and that the General Court' dismissal of the various arguments as to establish the necessity of the disclosure of the information was in breach of the principle of proportionality (par. 39).

The EDPS intervened before both Courts in favour of EFSA and against the applicants' limitation of the notion of personal data to the scope of privacy. The rights to privacy and protection of personal data are separate and the right to data protection applies whenever personal data are processed.

Main findings of the Court

On the concept of "personal data"

- ClientEarth and PAN Europe substantially requested to know the identity of the authors of each comment made by the external experts on the draft guidance document (par.28). As the information acquired would make it possible to connect a specific comment to a particular expert, the information itself constitutes a set of personal data within the meaning of Article 2(a) of Regulation No 45/2001, being it related to an identified natural person (par. 29).

"*In so far as that information would make it possible to connect to one particular expert or another a particular comment, it concerns identified natural persons and, accordingly, constitutes a set of personal data, within the meaning of Article 2(a) of Regulation No 45/2001*" (para 29).

- The characterization as personal data cannot be excluded: a) by the fact that the information is provided as a part of the professional activity (par. 30); b) by the circumstance that the identity of the experts and the comments were previously made public on the EFSA website; c) by the circumstance that the persons concerned do or do not object (par. 30-33).

On the conditions for transfer of personal data

- Where an application is made seeking access to personal data within the meaning of Article 2(a) of Regulation No 45/2001, the provisions of that regulation, and in particular Article 8(b) thereof, are applicable in their entirety (par.44)
- Under Article 8(b) of the Regulation No 45/2001, the transfer of personal data to recipients other than Community institutions and bodies is **cumulatively subjected to the necessity of the transfer, established by the recipient, and to the assumption of no prejudice for the legitimate interests of the data subject** (par. 45-46).
- The seeker of access shall establish the necessity of the transfer and then demonstrate it. The institution involved shall afterwards determine whether there is reason to assume that the transfer might jeopardize data subject's legitimate interests. In case it found no reason, then the access must be granted; conversely, if it founds reason for prejudice, it is for the institution to find the balance between the conflicting rights, as to establish whether to grant access or not (par. 47).
- As automatic priority cannot be conferred on the objective of transparency over the right to protection of personal data (judgment in *Volker und Markus Schecke and Eifert*, C-92/09 and C-93/09) the General Court held that the appellants had not established the necessity of the disclosure, since only a generic reference to the principle of transparency was made on their part (par. 51-52). A consideration of general nature is not sufficient in itself.
- The Advocate General argued that a lower requirement of necessity should be applicable in the case of professional activities.
- However, the Court noted that the appellants based their litigation on a precise accusation against EFSA, based on a precise study that showed that EFSA often retained experts linked to industrial lobbies (par. 53). Since the transparency of a decision-making process for the adoption of a measure as the guidance document (therefore with an impact on the activities of economic operators) contributes to that authority acquiring greater legitimacy towards the person directly involved, as well as accountability to citizens in a democratic system (par. 56), the acquisition of the information at issue was necessary so that the impartiality of these experts could be specifically assessed. Accordingly, the General Court was wrong to hold that the arguments of the parties were not sufficient to establish the necessity of the transfer (par. 59).

On the action before the General Court

- EFSA' allegation that the disclosure of the information would have been likely to undermine the privacy of the experts is based on a consideration of a general nature, not otherwise supported by any other specific element (par. 69).

> *(...) while the authority concerned* ***must assess whether the disclosure requested might have a specific and actual adverse effect on the interest protected*** *(...), EFSA's allegation that the disclosure of the information at issue would have been likely to undermine the privacy and integrity of the experts concerned* ***is a consideration of a general nature which is not otherwise supported by any factor which is specific to this case****. On the contrary,* ***such disclosure would, by itself, have made it possible for the suspicions of partiality in question to be dispelled or would have provided to experts who might be concerned with the opportunity to dispute, if necessary by available legal remedies, the merits of those allegations of partiality****.* (para. 69)

- Accepting such an unsupported claim by EFSA would mean it would apply to any situation where an authority of the European Union obtains opinion of experts prior to the adoption of a final measure having effects on economic operators. This outcome would be contrary to the requirement that exceptions to the right of access to documents held by the EU institutions must be interpreted strictly (par.70).
- Under Article 61(1) of the Statute of the CJEU when a judgment under appeal is set aside, the CJEU may issue final judgment in the matter if the state of the action permits the judgment. As the question of legitimate interest had not yet been considered at first instance, the Advocate General did not think that the state of the action permitted judgment by the Court of Justice. However the Court of Justice felt that the state of the action permitted it to set aside the judgment of the General Court and annul the decision of EFSA.

II. JUDGMENTS OF THE EUROPEAN COURT OF HUMAN RIGHTS

ARTICLE 8

1) Case n°68955/11, *Dragojević v. Croatia*, 15 January 2015 - Violation of Article 8 - Wiretapping of telephone conversations - surveillance orders insufficiently reasoned - lack of clarity of national law regarding the discretion of authorities

Link

Facts of the case

Mr Dragojevic, the applicant, is a Croatian national who works as a sailor on an ocean carrier for a shipping company based in Croatia.

In 2007, the police and the State Attorney's Office for the Suppression of Corruption and Organised Crime ('OSOC') investigated allegations of possible drug trafficking between Latin America and Europa via the ocean carrier and, therefore, requested an investigating judge of the Zagreb County Court to authorise the wiretapping of Mr Dragojevic's phone.

The same investigating judge issued successively four secret surveillance orders to tap the applicant's phone. The judge stated in particular that *"the investigation could not be conducted by other means"*. The applicant was under surveillance between 23 March and 7 August 2007 and subsequently from 17 September 2007.

Mr Dragojevic was arrested on 16 January 2009 and indicted with two other persons in the Dubrovnik County Court on charges of drug trafficking on 10 March 2009. The applicant pleaded not guilty and requested to have the results of the secret surveillance measures excluded from the case file, as unlawfully obtained evidence, on the grounds that the orders for their use had not been sufficiently reasoned.

On 18 December 2009, the Dubrovnik County Court dismissed his request, found Mr Dragojevic guilty and sentenced him to nine years' imprisonment. The judgment was based, among other things, on the use of the secret surveillance measures. Mr Dragojevic appealed the Court's decision with the Supreme Court and complained to the Constitutional Court, but in vain.

Main findings of the Court

- The Court started by reiterating that *"telephone conversations are covered by the notions of "private life" and " correspondence" within the meaning of Article 8"* and that *"their monitoring amounts to an interference with the exercise of one's rights under Article 8"* and then Court addressed both the requirements that this interference was "**in accordance with the law**" and that it was "**necessary in a democratic society**".
- The Court was satisfied that the measures had a basis in national law, namely the Croatian Code of Criminal Procedure.

- The central question was whether the system of secret surveillance, as applied by the Croatian authorities, had provided adequate safeguards against abuse. Having regard to the manner in which the Croatian courts had interpreted and applied the national law in Mr Dragojević's case, the Court found that **the law did not provide reasonable clarity as to the authorities' discretion in ordering surveillance measures and it did not in practice provide sufficient safeguards against possible abuse.**
- In reaching that conclusion, the Court noted that in Mr Dragojević's case the four secret surveillance orders issued by the investigating judge had essentially been based only on a statement referring to the prosecuting authorities' request for the use of such surveillance and the statutory phrase that "*the investigation could not be conducted by other means"*. **No details had been provided based on the specific facts of the case indicating a probable cause to believe that the offences had been committed and that the investigation could not be conducted by other, less intrusive, means.**
- Although that practice had been in conflict with the Code of Criminal Procedure and the case-law of the Croatian Constitutional Court – which expressly envisaged prior judicial scrutiny and detailed reasons when authorising secret surveillance orders – it had been approved by the Supreme Court. In an area as sensitive as the use of secret surveillance the Court had difficulty in accepting this situation.
- Moreover, as regards the possibility to challenge the lawfulness of the covert surveillance measures, the Court noted that in Mr Dragojević's case the criminal courts had limited their assessment of the use of secret surveillance to the question of whether the evidence thus obtained was to be admitted, without going into the substance of his allegations of arbitrary interference with his Article 8 rights.
- Finally, **the Croatian Government had not provided any information on remedies which would be available to a person in Mr Dragojević's situation.**
- Therefore the Court found that *"the relevant domestic law, as interpreted and applied by the competent courts, **did not provide reasonable clarity regarding the scope and manner of exercise of the discretion conferred on the public authorities**, and in particular did not secure in practice adequate safeguards against various possible abuse"* and concluded accordingly to a violation of Article 8.

2) Case n°30181/05, *Pruteanu v. Romania*, 3 February 2015 - Violation of Article 8 - Effective control over "lawyer-client" telephone recordings - lack of effective judicial redress

Link (only available in French)

Facts of the case

The applicant, Mr Pruteanu, is a Romanian national from Bacău and a lawyer.

A, B and her companion C are the partners of the commercial company M. located in Bacău. On 1 September 2004, the company M. was barred from carrying out bank transactions. The police received several criminal complaints against the company for deceit. The Public Prosecutor initiated criminal proceedings against both B and C (but not A). A took Mr Pruteanu as her lawyer.

On 24 September 2004, the District Court authorised the prosecuting authorities to intercept and record all the partners' telephone conversations for a period of 30 days. From 27

September to 27 October 2004, the fraud investigation unit intercepted and recorded A's conversations, including 12 conversations with her lawyer Mr Pruteanu.

On 21 March 2005, the District Court held that the recordings were relevant to the criminal case against B and C, and ordered that the transcripts and the tapes be placed under seal. Mr Pruteanu, on his own behalf, and A both lodged appeals. Mr Pruteanu asked for the deletion of those transcripts, **alleging that conversations between a lawyer and his client cannot be used as evidence in criminal proceedings**, and tried to challenge the legality of the interceptions, alleging that the taping of C.I.'s phone conversations is not based on legitimate grounds as she was not herself the subject of criminal proceedings. Those appeals were declared inadmissible.

Mr Pruteanu lodged an application against Romania in front of the European Court of Human Rights ('ECHR') complaining of an interference with his right to respect for his private life and correspondence on account of the recording of his telephone conversations with his client.

Main findings of the Court

- The ECHR first reiterated that telephone conversations are covered by the notions of "private life" and "correspondence" within the meaning of Article 8 § 1 of the Convention and therefore their interception amounts to an "interference by a public authority" with the exercise of one's rights under Article 8. The fact that the telephone tapping in question was carried out on the telephone line of a third party is of little importance in that regard.
- The Court analysed whether or not the interference is **necessary in a democratic society**.
- Whatever system of surveillance is adopted, **adequate and effective guarantees against abuse** must be provided, which depends *inter alia* on the kind of remedies provided by the national law. The Court had therefore to examine the procedures for supervising the ordering and implementation of the interfering measures.
- The Court first noted that the authorisation to record the telephone conversations of A given by the District Court targeted A, and not the applicant, in such a way that it cannot be concluded that the District Court had examined *a priori* the necessity of this measure towards the applicant. The Court then examined if the applicant had any remedy available *a posteriori* in order to exercise an **effective control** over the telephone recordings contested.
- When analysing the legislation in force at the time of the facts, **the Court concluded that the applicant did not have any legal grounds to intervene on his own behalf in the criminal proceedings in which the recordings were used.** Therefore, the applicant could not exercise control of the lawfulness and the necessity of the recordings, nor could he require a balance between the interest of justice and his rights to respect for private life and correspondence.
- Considering that the only way the applicant could have challenged the lawfulness of the interceptions was during a criminal trial against himself or against his client, the Court concluded that the accessibility of a remedy for the applicant was uncertain.
- As regards a civil action to ask for damages (which was pointed out by the Government as an alternative), the Court stated that the Government did not provide any example of case law which would prove the effectiveness of this particular remedy. In addition, a complaint in front of a civil judge regarding the pecuniary liability of the State does not have the nature to allow the control of the legality of the recordings and to lead, where

appropriate, to a decision that orders their deletion – a result sought by the applicant –, so as it could not be seen as an effective control for the purposes of Article 8.

- The Court concluded to the violation of Article 8 considering that the interference was disproportionate and the applicant had not have access to an effective control in order to limit this interference to what is necessary in a democratic society.

3) Case n°5678/06, *Yuditskaya and Others v. Russia*, 12 February 2015 - Violation of Article 8 - Search of a law firm - attorney-client confidentiality privilege

Link

Facts of the case

The applicants are five Russian nationals, all members of the Perm Bar and lawyers with the 'Biznes i Pravo' law firm.

On 1 December 2004, a criminal investigation was opened into bribe-taking by court bailiffs. The Russian Government suspected that the director of the Kirov Perm Factory, K., had bribed a bailiff and that the bagman for the bribe cash had been bailiff T. In order to legalise the transaction, bailiff T. had asked his brother I.T., lawyer at the 'Biznes i Pravo' law firm, to sign a fictitious legal assistance contract with the Factory in respect of legal advice on tax.

On 6 May 2005, the Disctrict Court of Perm issued a search warrant authorising the search of the law firm. On 16 May 2005, all the offices of the law firm, including I.T.'s office but also the offices of the five applicants who had no relationship with the Factory, were searched. The investigators took away all the computers for a week and meanwhile copied the entire contents of their hard disks.

The applicants appealed the decision of the District Court alleging that there had been no grounds for searching the entire premises of the law firm and referring to the fact that the search and seizure of their computers, which were protected by the attorney-client privilege, was a gross violation of the Advocates Act. Their appeal was dismissed by the Regional Court on 23 June 2005.

Main findings of the Court

- The Court reiterated that *"the search of the applicants' legal offices and the seizure of their computers constituted an interference with their right to respect for "private life", "home" and "correspondence""* before analysing if the measure was "**necessary in a democratic society**".
- To this end, the Court explored the availability of **effective safeguards** against abuse or arbitrariness under domestic law and checked how those safeguards operated in this case.
- The Court considered that the search warrant was not **based on reasonable suspicion**, as the applicants were not the subjects of any criminal investigation (only I.T. was). Furthermore, the Court considered that the **scope of the warrant** was not **reasonably limited**, as it was drafted in very broad terms, giving the investigators unrestricted discretion in the conduct of the search and since the Russian judge did not touch upon the issue of whether privileged material was to be safeguarded.
- Having regard to the materials inspected and seized, the Court observed that the warrant's excessive breadth was reflected in the way in which it was executed and noted that **no**

safeguard were put in place to prevent interference with professional secrecy (e.g. the presence of an independent observer capable of identifying documents covered by privilege during the search).

- Therefore, the Court considered that the search carried out went beyond what was "necessary in a democratic society" to achieve the legitimate aim pursued and concluded to a violation of Article 8 of the Convention.

4) Case n°45797/009, *Zaichenko v. Ukraine* (No 2), 26 February 2015 - collection of information by the police forces for the purpose of a psychiatric examination

Link

Facts of the case

The applicant wrote letters to the Regional Administrative Court which contained rude remarks about the judges involved in his cases. Consequently, the court drew a report stating that the applicant was in contempt of court. Hearing this case, the District Court ordered a forensic psychiatric examination and later instructed the police to collection information on the applicant's personality, which was required for the psychiatric hospital to carry out the examination. In particular, the police was asked to collect any documentation relating to psychiatric treatment or drug therapy received by the applicant, as well as character references for him from his relatives, neighbours and colleagues.

After pursuing national remedies, the applicant brought a complaint in front of the ECHR alleging that his right to liberty was violated by his involuntary confinement in a psychiatric hospital and alleging that the collection of information about him by the police without his consent violated Article 8.

Main findings of the Court

- The Court reiterated that "the collection and storage of information relating to an individual's private life or the release of such information" fall under Article 8 § 1. (§ 117)
- The Court also recalled that a measure must have a basis in domestic law and must be compatible with the rule of law to be considered "in accordance with the law". "The law must be adequately accessible and foreseeable, that is, formulated with sufficient precision to enable the individual to regulate his conduct". Domestic law must thus "afford adequate legal protection against arbitrariness and accordingly indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise". (§ 118)
- At the time of the alleged violation, the relevant national provision had not been amended since it was enacted therefore the Court drew attention to the criticisms of the Constitutional Court in that regard. (§ 119)
- The Constitutional Court had criticised the fact that "the issues of collection, storage, use and dissemination of information about individuals, in particular, about their mental state and mandatory psychiatric examination or treatment" were not sufficiently regulated. It also denounced the lack of a "procedure for the protection of individuals' rights against the unlawful interference of psychiatric services in their private life". (§ 68)

- The Court also referred to the **lack of necessary safeguards against arbitrariness in respect of forensic psychiatric examinations in the context of administrative proceedings**. (§§ 101 and 120)
- The Court held that those findings were sufficient to declare that the interference with the applicant's private life was unlawful (§§ 121).

Conclusion: There is a violation of Article 8.

5) Case n°28005/12, *M.N. v. San Marino*, 7 July 2015 - lack of safeguards related to a decision to copy and store bank documents - "copying" data amounts to "seizure" of data - ordinary civil remedy against the State is not "effective review"

Link

Facts of the case

Following a request of the Italian authorities related to an ongoing investigation into money laundering, the San Marino court ordered an investigation to collect information and banking documents related to accounts linked to a San Marino company. The search and seizure activities involved the retention of copies of the documentation and of electronic storage devices, including e-mails, bank statements and cheques. A second order required Italian citizens who had entered fiduciary agreements with the company to be notified of the decision of the court. The applicant was affected by the decision and was informed about it. As a result, he lodged a complaint with the San Marino court on the grounds that he had never been charged with an offence and had no link with the alleged crimes. He also complained that his right of appeal was violated because he lacked standing due to the fact that he was not charged with an offence.

Main findings of the Court

Admissibility

- The Court held that information retrieved from banking documents amounts to personal data concerning an individual, whether or not it constitutes sensitive information or professional dealings (§ 51).
- **The Court confirmed that Article 8 is applicable in the context of seizures of professional documents and personal data.** Moreover, the storage of such data constitutes interference "irrespective of who is the owner of the medium on which the information is held". Storing and releasing information related to private life while refusing the individual an opportunity to contest it constitutes interference under Article 8. (§ 53)
- The Court added that "copying" amounts to the seizure of data "'irrespective of the fact that the original medium may have remained in place" and it held that the copying also led to the immediate and independent storage of such data. (§ 54)
- The seizure and the storage by the authorities of the bank data amounts to interference for the purposes of Article 8 therefore the case is admissible. (§ 55)

Substance

- First, the Court found that the interference was prescribed by law because legislation provided for an exception to the right of banking secrecy when measures were taken by judicial authorities in criminal proceedings and the Code of Criminal Procedure stated that those measures could extend to third parties. (§ 74)
- The Court also held that the measure pursued several legitimate aims - "the prevention of crime, the protection of the rights and freedoms of others, and also the economic well-being of the country". (§ 75)
- In assessing whether the measure was necessary in a democratic society, the Court characterised the order to collect information and banking documents as wide because it also had an impact on third parties not subject to the investigation. Moreover, the Court noted that, even if the San Marino Court had the power to make the order, it failed to assess the need for such an order. (§ 77)
- In assessing whether relevant procedural safeguards were put in place, the Court examined "whether an effective control was available to the applicant to challenge the measure to which he had been subjected (...) and therefore whether subsequent to the implementation of that order the applicant had available any means for reviewing it". (§ 78)
- The Court noted that the applicant was made aware of the order following a later order to notify the parties affected. After being notified with delay, the applicant brought proceedings for which he was refused standing because he was not an "interested person". (§ 79)
- In that regard, the Court held that "the institution of proceedings does not, in itself, satisfy all the access to court requirements of Article 6§1" therefore this is not sufficient to fulfil the requirement of effective control. (§ 80)
- The Court further ruled that the Government **failed to show that an ordinary civil remedy was available to the applicant**. **In any event, it would not have qualified as ''effective review'' for the purposes of Article 8 because a claim for damages against the State in ordinary proceedings is distinct from an application for judicial review since only the latter can annul the contested measure.** (§ 81)
- In light of the fact that no other procedure was available to the applicant and that he "was at a significant disadvantage in the protection of his rights compared to an accused person (...)", he was not effectively protected by national law. As a result, he did not have **''effective control to which citizens are entitled under the rule of law and which would have been capable of restricting the interference in question to what was necessary in a democratic society''**. (§ 83)

Conclusion: There is a violation of Article 8.

6) Case n°62498/11, *R.E. v. United Kingdom*, 27 October 2015 - Covert surveillance of a detainee's consultations with his lawyer and with the person appointed to assist him, as a vulnerable person, following his arrest - legal consultations are stricter protected under Article 8, than consultations with appropriate adult[4]

Link

Facts of the case

[4] Official HUDOC Summary.

Part II of the Regulation of Investigatory Powers Act 2000 (RIPA) combined with the Covert Surveillance Code of Practice permits covert surveillance in certain circumstances.
Between 15 March 2009 and 8 May 2010 the applicant, an Irish national, was arrested and detained three times in connection with the murder of a police officer believed to have been killed by dissident Republicans. When first arrested he was assessed by a medical officer as being mentally vulnerable, which meant that he could not be interviewed in the absence of an appropriate adult (a relative or guardian). During the first two periods of detention his solicitor received assurances from the Police Service of Northern Ireland (PSNI) that his consultations with the applicant would not be subject to covert surveillance.
The applicant was arrested for the third time on 4 May 2010 before being released, without charge, four days later. On this occasion, the PSNI refused to give an assurance to his solicitor that their consultations would not be subject to covert surveillance. An application by the applicant for judicial review of that decision was dismissed in September 2010 after the High Court ruled that the statutory provisions governing covert surveillance were clearly defined and sufficiently detailed and precise.

Main findings of the Court

- The Court proceeded on the basis that there had been an interference with the applicant's right to respect for his private life. The interference pursued the legitimate aims of protecting national security and preventing disorder and crime. It had a basis in domestic law (RIPA and the Covert Surveillance Code of Practice), which law was sufficiently accessible. In view of their similarity in the special context of secret surveillance measures, the issue whether the domestic law was also adequately foreseeable was addressed jointly with the question whether the interference had been necessary in a democratic society.

(a) Surveillance of legal consultations

- The Government had argued that under the Court's case-law less stringent safeguards were required in covert surveillance cases (such as the applicant's) than those the Court had laid down in interception-of-communication cases such as Weber and Saravia v. Germany and, in relation to Part I of RIPA, Kennedy v. the United Kingdom. The Court observed, however, that the decisive factor was not the technical definition of the interference, but the level of interference with the right to respect for private life.
- **The surveillance of legal consultations constituted an extremely high degree of intrusion and was analogous to the interception of a telephone call between a lawyer and client.** Article 8 afforded "strengthened protection" to exchanges between lawyers and their clients, as lawyers would be unable to defend their clients if they were unable to guarantee that their exchanges would remain confidential. Consequently, the same safeguards from arbitrary interference were required for surveillance of legal consultations as in interception-of-communications cases, at least insofar as those principles could be applied to the form of surveillance in question.
- The Court found that the relevant provisions were sufficiently clear as regards (i) the nature of the offences that could give rise to covert surveillance, (ii) the categories of persons liable to such surveillance and (iii) the duration, renewal and cancellation of the surveillance measures. However, it was not satisfied that the provisions of Part II of RIPA and Covert Surveillance Code of Practice provisions afforded persons

affected by the surveillance of legal consultations **with sufficient safeguards as regards the examination, use and storage of the material, the precautions to be taken when communicating the material to other parties, and the circumstances in which recordings were to be erased or the material destroyed.** These provisions were to be contrasted with the more detailed provisions of Part I of RIPA and the Interception of Communications Code of Practice which the Court had approved in Kennedy. Further, although a new service procedure (the Police Service of Northern Ireland Service Procedure, 'Covert Surveillance of Legal Consultations and the Handling of Legally Privileged Material') had since put in place further safeguards for the secure handling, storage and destruction of material obtained through covert surveillance, it was not in force during the applicant's detention in May 2010.

- Consequently, during the relevant period of the applicant's detention the impugned surveillance measures, insofar as they may have been applied to him, had not met the requirements of Article 8 § 2 of the Convention as elucidated in the Court's case-law.

Conclusion: violation of Article 8.

(b) Surveillance of consultations between detainee and appropriate adult

- The surveillance of consultations between a vulnerable detainee and an appropriate adult appointed to assist him or her following arrest also constituted a significant degree of intrusion. However**, the surveillance did not take place in a private place, but in a police station and, unlike legal consultations, consultations with an appropriate adult were not subject to legal privilege and did not attract the "strengthened protection" accorded to consultations with lawyers or medical personnel.** The detainee would not, therefore, have the same expectation of privacy as during a legal consultation. The Court therefore applied a less strict standard and focused on the more general question of whether the legislation adequately protected detainees against arbitrary interference with their Article 8 rights and was sufficiently clear in its terms to give individuals an adequate indication as to the circumstances in which and the conditions on which public authorities were entitled to resort to covert measures.
- The Court concluded that the provisions concerning the possible surveillance of consultations between vulnerable detainees and appropriate adults had been accompanied by adequate safeguards against abuse. In this connection it noted that: authorisations for surveillance had to be regularly reviewed and were cancelled if the criteria were no longer met; authorisation could only be granted for three months at a time and detailed records of all authorisations had to be kept; the scheme was supervised by surveillance commissioners; the admissibility of evidence obtained through surveillance was subject to the control of the trial judge; and aggrieved parties could bring a claim to the Investigatory Powers Tribunal, which had power to award compensation, to quash or cancel orders and to order the destruction of any records.

Conclusion: no violation of Article 8.

7) Case n°47143/06, *Roman Zakharov v. Russia*, 4 December 2015 - interceptions of communications interfering with Article 8 ECHR

Link

Facts of the case[5]

Zakharov, a publisher and a chairman of an NGO campaigning for media freedom and journalists' rights, sought to challenge the Russian system for permitting surveillance in the interests of crime prevention and national security. Z claimed that the privacy of his communications across mobile networks was infringed as the Russian State, by virtue of Order No. 70, had required the network operators to install equipment which permitted the Federal Security Service to intercept all telephone communications without prior judicial authorisation.

This facilitated blanket interception of mobile communications. Attempts to challenge this and to ensure that access to communications was restricted to authorised personnel were unsuccessful at national level. The matter was brought before the European Court of Human Rights. He argued that:

- the laws relating to monitoring infringe his right to private life under Article 8;
- that parts of these laws are not accessible; and
- that there are no effective remedies (thus also infringing **Art. 13 ECHR**).

Main findings of the Court

Admissibility

- The applicant claimed that his right was infringed as a result of the mere existence of the legislation in question. However, the Court's role is not to review legislation *in abstracto* and **applicants must show that they are directly affected by the contested measure pursuant to Article 34.** (§§ 163-164)
- Nonetheless, the Court previously held in *Klass and Others v. Germany* that **"an individual might, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures, without having to allege that such measures had been in fact applied to him**". (§ 165)
- To clarify the two approaches later developed in its case-law, the Court stated the conditions to be fulfilled (§§ 166-172):
  - **the applicant can possibly be affected by the scope of the legislation; and**
  - **the national remedies are either unavailable or ineffective.**
- In the present case, the Court held that "[h]aving regard to the secret nature of the surveillance measures provided for by the contested legislation, the broad scope of their application, affecting all users of mobile telephone communications, and the lack of effective means to challenge the alleged application of secret surveillance measures at domestic level, (...) an examination of the relevant legislation in abstracto to be justified. (...) **the applicant is entitled to claim to be the victim of a violation of the**

[5] Summary of the facts made by Prof. Woods available here.

Convention, even though he is unable to allege that he has been subject to a concrete measure of surveillance in support of his application. For the same reasons, **the mere existence of the contested legislation amounts in itself to an interference with the exercise of his rights under Article 8**." (§§ 178-179):

Substance

- In assessing whether the interference was in accordance with the law, the Court first noted that most legal provisions relating to secret surveillance are accessible to the public. Regarding the order describing the technical requirements of the equipment to be installed by the service providers, the Court held that it must be accessible to the public because it also required the providers to give law enforcement authorities direct access to all communications and mandated not to record the interceptions. Although the Court stated that it found this regrettable, it chose not to analyse the issue further in light of the fact that the order had been published in a specialised magazine and on an internet legal database. (§§ 239-242)
- Next, the Court indicated that a law is foreseeable where the rules are sufficiently detailed and clear so as to enable citizens to have "an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to [the interception of telephone conversations]". (§§ 229)
- Moreover, "the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference". (§§ 230)
- The Court recalled the minimum safeguards to be included in the law in order to avoid abuses of power:
    - **the nature of offences which may give rise to an interception order;**
    - **a definition of the categories of people liable to have their telephones tapped**
    - **a limit on the duration of telephone tapping;**
    - **the procedure to be followed for examining, using and storing the data obtained;**
    - **the precautions to be taken when communicating the data to other parties; and**
    - **the circumstances in which recordings may or must be erased or destroyed.** (§§ 231)

1) Scope of application of the measures: the circumstances in which public authorities are empowered to resort to secret surveillance measures are not defined with sufficient clarity.

- Although Russian law indicates with sufficient clarity the nature of the offences which may give rise to the interception of communications, it covers a wide range of offences. It may also be ordered in respect of "a person who may have information about an offence or may have other information relevant to the criminal case" without defining those terms. (§§ 244-245)
- Moreover, interception is also allowed "following the receipt of information about events or activities endangering Russia's national, military, economic or ecological security" without those terms being defined. The Court found that this "leaves the authority an almost unlimited degree of discretion in determining which events or acts constitute such a threat and whether that threat is serious enough to justify secret surveillance, thereby creating possibilities for abuse". (§§ 246-248)

2) Duration of the measures: provisions on discontinuation of secret surveillance measures do not provide sufficient guarantees against arbitrary interference.

- The Court held that adequate domestic safeguards must include "the period after which an interception warrant will expire, the conditions under which a warrant can be renewed and the circumstances in which it must be cancelled". However, the legislative framework dealing with interception outside of criminal proceedings does not include a requirement to discontinue the surveillance when no longer necessary. (§§ 250-251)

3) Procedures to be followed for storing, accessing, examining, using, communicating and destroying the intercepted data: the domestic law permitting automatic storage of clearly irrelevant data is not sufficiently clear as to the circumstances in which the intercept material will be stored and destroyed after the end of a trial.

- Where the person concerned has not been charged with a criminal offence, the Court held that the storage of intercepted data for a 6-month period is reasonable. However, the automatic storage of data irrelevant for the purpose for which they were obtained cannot be justified under Article 8. (§§ 254-255)
- Where the person concerned has been charged with a criminal offence, the trial judge has unlimited discretion to store the data used at the end of the trial because the law does not indicate the circumstances under which it should be stored or destroyed. (§ 256) Therefore, the law is not sufficiently clear as to the circumstances in which the intercept material will be stored and destroyed after the end of a trial.

4) Authorisation of interceptions: the authorisation procedures are not capable of ensuring that secret surveillance measures are ordered only when "necessary in a democratic society".

- **Authorisation procedures should ensure that ''secret surveillance is not ordered haphazardly, irregularly or without due proper consideration**''. (§ 257)
- The Court first assessed whether the authority competent to authorise the surveillance is "sufficiently independent from the executive". In Russia, the authorisation must be reasoned and granted by a court. (§§ 258-259)
- Secondly, the scope of review of the authority "must be capable of verifying the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures". In addition, the authority must also assess whether the surveillance is necessary in a democratic society. (§ 260)
- Although surveillance must be authorised by a court under Russian law, the judicial scope of review is limited because materials relating, amongst others, to operational-search measures and undercover agents are excluded from the scope. As a result, the competent authority cannot assess whether there are factual indications justifying that the person concerned be suspected. Moreover, the Court found that the authorities are not obliged to determine whether there is a reasonable suspicion or to assess the proportionality and necessity of the measure. (§§ 261-263)
- Thirdly, the Court analysed the content of the authorisation. It denounced the fact that some authorisations do no mention the specific person to be placed under surveillance nor the duration for which it is granted. Moreover, an urgency procedure allows for a very

wide discretion of the law enforcement authorities and does not provide for effective judicial review. (§§ 264-266)

- Finally, the Court held that the Russian system of surveillance which allows the secret services and law enforcement authorities to access the communications directly without authorisation is "particularly prone to abuse" therefore strong safeguards must exist. (§ 270)

5) Supervision of the implementation of the measures: the supervision of interceptions, as it is currently organised, does not comply with the requirements of independence, powers and competence which are sufficient to exercise an effective and continuous control, public scrutiny and effectiveness in practice.

- The Court held that the supervision is ineffective because the communications service providers are prohibited from logging the interception activities and the law enforcement authorities can intercept the communications directly without requesting authorisation to do so. (§ 272)
- The Court also pointed out that the judicial supervision is limited to the initial authorisation whereas the supervision of its implementation is left to the President, Parliament, Government, the Prosecutor General and competent lower-level prosecutors. It went on to assess whether those supervisory bodies are "independent of the authorities carrying out the surveillance" and "vested with sufficient powers and competence to exercise an effective and continuous control". (§§ 274-275)
- Although Russian law sets out the rules regarding the supervision by prosecutors, their appointment and dismissal by the Prosecutor General may affect their independence and conflicts of interests may arise because they also grant the interception authorisations in the first place. Moreover, information relating to the secret services is outside the scope of review. (§§ 276-281)
- Finally, the activities of the supervisors are not open to public scrutiny. (§ 283)

6) Notification of interception and available remedies: the effectiveness of the remedies is undermined by the absence of notification at any point of interceptions, or adequate access to documents relating to interceptions.

- The Court highlighted that remedies are only available to those who have been informed about the interception of their communications. Where no criminal proceedings are brought against the person concerned, there is no effective judicial remedy because there is no notification obligation or an "adequate possibility to request and obtain information about the interceptions". (§ 298)

Conclusion: For the above reasons, the Court concluded that Russian law does not provide for "**adequate and effective guarantees against arbitrariness and the risk of abuse which is inherent in any system of secret surveillance, and which is particularly high in a system where the secret services and the police have direct access, by technical means, to all mobile telephone communications**."

8) Case n° 37138/14, *Szabó and Vissy v. Hungary*, 12 January 2016 - legislation on anti-terrorist secret surveillance

Link

Facts of the case

In 2011, Hungary passed a law on secret anti-terrorist surveillance. The applicants, staff members of a non-governmental organisation, complained that they could potentially be subjected to unjustified and disproportionately intrusive measures. Under the new legislation, an Anti-Terrorism Task Force has large secret intelligence prerogatives, including checking and recording contents of electronic or computerised communications, without the consent of the persons concerned. Secret surveillance in order to prevent terrorist acts or in the interests of national security is authorised by the Minister of Justice.

Main findings of the Court

- First, the scope of the legislation includes anyone in Hungary and it cannot be excluded that the applicants are at risk of being subjected to these measures.
- Then, the Court admitted that as a consequence of present-day terrorist attacks, government may attempt to prevent terrorist acts, including with massive monitoring of communications.
- However, the legislation did not provide sufficient safeguards against abuse of monitoring powers.
- The Court noted the absence of notification to the person concerned after the termination of the surveillance measure and of any formal remedies in case of abuse.
- Furthermore, surveillance measures are ordered by the executive branch and without any assessment of strict necessity while the government has the possibility to intercept masses of data easily concerning even persons outside the original range of operation.

Conclusion: The Court held that there had been a **violation of Article 8** of the Convention.

ARTICLE 10

1) Case n°64569/09, Delfi v. Estonia, 16 June 2015, Grand Chamber - civil liability of a news portal for users' comments on its articles - importance of anonymity on the Internet - degrees of anonymity

Link

[Official HUDOC summary of facts and main findings]

This was the first case in which the Court had been called upon to examine a complaint about liability for user-generated comments on an Internet news portal. The applicant company, Delfi AS, which runs a news portal run on a commercial basis, complained that it had been held liable by the national courts for the offensive comments posted by its readers below one of its online news articles about a ferry company. At the request of the lawyers of the owner of the ferry company, Delfi removed the offensive comments about six weeks after their publication.

The case therefore **concerned the duties and responsibilities of Internet news portals** which provided on a commercial basis a platform for user-generated comments on previously published content and some users – whether identified or anonymous – engaged in clearly unlawful hate speech which infringed the personality rights of others. The Delfi case **did not**

concern other fora on the Internet where third-party comments could be disseminated, for example an Internet discussion forum, a bulletin board or a social media platform.

The question before the Grand Chamber was not whether the freedom of expression of the authors of the comments had been breached but **whether holding Delfi liable for comments posted by third parties had been in breach of its freedom to impart information**. The Grand Chamber found that the Estonian courts' **finding of liability against Delfi had been a justified and proportionate restriction on the portal's freedom of expression**, in particular, because: the comments in question had been extreme and had been posted in reaction to an article published by Delfi on its professionally managed news portal run on a commercial basis; the steps taken by Delfi to remove the offensive comments without delay after their publication had been insufficient; and the 320 euro fine had by no means been excessive for Delfi, one of the largest Internet portals in Estonia.

Particularly interesting findings of the Court regarding anonymity:

- Within its reasoning, the Court assessed whether the liability of the actual authors of the comments could serve as a sensible alternative to the liability of the Internet news portal. (§ 147)
- To answer above question, the Court admitted it is "mindful the Court is mindful of the interest of Internet users in not disclosing their identity. **Anonymity has long been a means of avoiding reprisals or unwanted attention. As such, it is capable of promoting the free flow of ideas and information in an important manner, including, notably, on the Internet**." (§ 147)
- The Court balanced this finding with "the ease, scope and speed of the dissemination of information on the Internet, and the persistence of the information once disclosed, which may considerably aggravate the effects of unlawful speech on the Internet compared to traditional media" and referred to CJEU C-131/12, *Google v. Spain*. (§ 147)
- Further, the Court observed that "**different degrees of anonymity are possible on the Internet**". (§ 148)
- It went on to differentiate these degrees of anonymity:
    - **1st degree**: "An Internet user may be anonymous to the wider public while being identifiable by a service provider through an account or contact data that may be either unverified or subject to some kind of verification – ranging from limited verification (for example, through activation of an account via an e-mail address or a social network account) to secure authentication, be it by the use of national electronic identity cards or online banking authentication data allowing rather more secure identification of the user".
    - **2nd degree**: "A service provider may also allow an extensive degree of anonymity for its users, in which case the users are not required to identify themselves at all and they may only be traceable – to a limited extent – through the information retained by Internet access providers. The release of such information would usually require an injunction by the investigative or judicial authorities and would be subject to restrictive conditions. It may nevertheless be required in some cases in order to identify and prosecute perpetrators". (§ 148)
- Because proof from the Estonian government showed that "in some cases has proved possible to establish the computer from which the comments had been made, while in

other cases, for various technical reasons, this has proved impossible", the Court considered that "the uncertain effectiveness of measures allowing the identity of the authors of the comments to be established, coupled with the lack of instruments put in place by the applicant company for the same purpose with a view to making it possible for a victim of hate speech to effectively bring a claim against the authors of the comments" support the national court's conclusion that the news portal must be held liable in this case. (§ 151)

2) Case n°931/13, *Satamedia v. Finland*, 21 July 2015 *(request for referral to the Grand Chamber pending)* - whether the publication of taxation information falls under the journalistic exception

Link

Facts of the case

The first applicant company issues a magazine which publishes yearly information about natural persons' taxable income and assets. In 2002, the magazine appeared 17 times and published data on 1.2 million citizens, which representing a third of all taxable persons in Finland. The second applicant company, owned by the same person, offers an SMS-service which provides taxation information found in a database built using the information published in the magazine when a person sends a person's name.

Following a preliminary reference to the CJEU asking whether the activities pursued by the companies constituted "processing of personal data" to which the Directive 95/46 applied, the Supreme Administrative Court request the Data Protection Board to prohibit the processing of taxation data in the manner and to the extent carried out in 2002. The Board prohibited the first applicant company to process taxation data in this manner and to forward it to an SMS-service while forbidding the second applicant company to collect, save or forward to an SMS-service any information received from the magazine.

The applicant companies appealed the decisions up to the Supreme Administrative Court but failed in doing so. They complained in front of the ECHR that Article 10 had been violated in a manner which was not necessary in a democratic society.

Main findings of the Court

- The Court found that the Data Protection Board did not prohibit the publication of taxation data. However, there was an interference with the companies' right to impart information because they were, instead, prohibited from **''collecting, saving and processing such data to a large extent''** therefore they could not publish an essential part of the content previously published in the magazine. (§ 53)
- The Court held that the Personal Data Act, which includes the journalistic exception, provided for the interference therefore it was prescribed by law. Moreover, the interference "pursued the legitimate aim of protecting the reputation or rights of others". (§ 55)
- After restating its case-law, the Court stressed that, in order to determine whether the interference was necessary in a democratic society, it must assess whether the interference was "proportionate to the legitimate aims pursued" and whether the justifications were "relevant and sufficient". (§ 59)

- The Court reiterated that the press has a duty to impart "information and ideas on all matters of public interest" and the public has a right to receive them. (§ 60)
- As already held in *Von Hannover* and *Axel Springer*, the following criteria need to be taken into account by the Court in assessing whether the domestic authorities struck a fair balance between freedom of expression and the right to respect for private life:
    - "**(i) contribution to a debate of general interest;**
    - **(ii) how well-known is the person concerned and what is the subject of the report;**
    - **(iii) prior conduct of the person concerned;**
    - **(iv) method of obtaining the information and its veracity/circumstances in which the photographs were taken;**
    - **(v) content, form and consequences of the publication; and**
    - **(vi) severity of the sanction imposed**." (§ 62)
- The Court noted that the taxation data was public therefore it was justified to impart this information to the public. (§ 65) The information was obtained legally and there was no doubt as to its accuracy. (§§ 66-67)
- According to the domestic authorities, the issue focused on the extent of the information published. The national courts found that such an extent could not be considered as journalism and the Supreme Administrative Court referred the question to the CJEU. (§ 68)
- The CJEU held that journalism must be interpreted broadly in light of the right to freedom of expression. However, derogations and limitations to the right to protection of personal data provided in the Directive must apply only in so far as strictly necessary to achieve a balance between the competing rights. The CJEU ruled that the activities of the companies could be considered journalistic "if their object was to disclose to the public information, opinions or ideas, irrespective of the medium which was used to transmit them". (§ 69)
- In light of the ruling, the Supreme Administrative Court held that "the public interest did not require such publication of personal data to the extent that had been seen in the present case, in particular as the derogation in the Personal Data Act was to be interpreted strictly". (§ 70)
- The Court held that this reasoning was "acceptable" and took into account the Court's case-law. (§ 72)
- The Court also noted that the companies were not prohibited from publishing the information altogether and that they could have published it to a lesser extent. "**The fact that, in practice, the limitations imposed on the quantity of the information to be published may have rendered the applicant companies' business activities unviable is not, however, a direct consequence of the actions taken by the domestic courts and authorities but an economic decision made by the applicant companies themselves**''. (§ 73)

Conclusion: There is no violation of Article 10.

3) Case n°4054/07, *Couderc and Hachette v. France*, 10 November 2015 - right to private life balanced against freedom of expression

Link

Facts of the case

A French tabloid published an article on the illegitimate son of Albert de Monaco with pictures of the Prince holding his son. The article described how the mother met the Prince, their intimate relationship, their feelings, and how he reacted to the new of the pregnancy and behaved regarding his son. The French Court of Appeal ordered the magazine to pay 50.000 euros to the Prince for breach of his right to privacy and to protection of his own image. The Court of Cassation confirmed that "every person, whatever his rank, birth, fortune or present or future functions, is entitled to respect for his private life" especially regarding the lack of any topical news item or any debate on a matter of public interest.

Main findings of the Court

The Court found **a violation of Article 10 of ECHR**. The article and interview of the mother were part of a debate of general interest, in particular regarding the hereditary nature of the dynasty. The interests of the mother and the child were also at stake in asserting his existence and having his identity recognized by the Prince.

Conclusion: Preventing the disclosure of information on the Prince's private life constitutes a strong interference with the undeniable public-interest value in the existence of a son.

4) Case n°3690/10, *Annen v. Germany*, 26 November 2015 - right to private life balanced against freedom of expression

Link

Facts of the case

An abortion opponent distributed leaflets in the immediate vicinity of a clinic stating the names and addresses of two doctors practicing "unlawful" abortion there. He also had a website called babycaust.de listing the names of doctors practicing abortion in Germany.
The clinic doctors obtained a civil injunction ordering the opponent to stop disseminating in the immediate vicinity the leaflets and listing the names of the doctors on his website. His statements made the incorrect allegation that abortions were performed outside the legal conditions. The Court applied the same principles to the publication of the doctors' names on the website, which title also implied a connection between them and the crimes committed by the Nazis during the Holocaust.
The opponent complained that the civil injunction violated his right to freedom of expression.

Main findings of the Court

Prohibiting an abortion opponent from distributing leaflets and publishing the names of doctors practicing abortion on a website violates his right to freedom of expression protected by Article 10 of ECHR. The German courts had failed in finding a fair balance between this right, addressing questions of public interest, and the doctors' rights. In particular, the leaflets

stated in small letters that abortions were allowed in Germany. Thus, it was made clear that the abortions performed in the clinic were not subject to criminal liability.
Moreover, despite the reference to the Holocaust, the opponent did not compare the doctors' activities to the Nazi regime and did not explicitly equate abortions with the Holocaust.

Conclusion: Freedom of expression applies not only to inoffensive information or ideas but also to those that offend, shock or disturb. However, it can be restricted to protect the rights of others, including their right to the protection of their reputation, protected under Article 8. Here, the interference was necessary in a democratic society.

III. SELECTED CASES FROM NATIONAL COURTS

1) *Vidal-Hall, Hann and Bradshaw v Google Inc* [2015] EWCA Civ 311, 27 March 2015 - Browser Generated Information - Moral damages for breach of data protection law recognised - Misuse of personal data recognised as distinct cause of action

Link

Facts of the case:

Google collected private information about the claimants' internet usage via their Apple Safari browser (i.e. Browser Generated Information, hereinafter referred to as 'BGI'), without the claimants' knowledge and consent, by means of cookies. The private information was aggregated and used to create targeted ads based on the claimants' profile, which were displayed on their computer. The ads revealed private information and were seen or might have been seen by third parties. This practice was contrary to the publicly stated position of Google regarding Safari users. The claimants allege, in respect of their claims for misuse of private information and/or breach of confidence, that their personal dignity, autonomy and integrity were damaged, and claim damages for anxiety and distress.

The key-issue was to establish, first, whether the Courts in England had jurisdiction to decide on this case, since the claimants are domiciled in England and the defendant is based in California). The rationale which allows a "claim out of jurisdiction" also solves, on substance, the case.

The summarized decision was given in Appeal.

In first instance, the Court had decided that the claimants can serve the claim on Google out of jurisdiction, following the Civil Procedure Rules.

Relevant provisions

General conditions to grant a request to serve the claim out of jurisdiction	The claimants had to establish: (i) that there was a serious issue to be tried on the merits of their claims; i.e. that the claims raised substantial issues of fact or law or both; (ii) that there was a good arguable case that their claims came within one of the jurisdictional 'gateways' set out in CPR PD 6B (Civil Procedure Rules Practice Direction 6 B); (iii) that in all the circumstances, England was clearly or distinctly the appropriate forum for the trial of the dispute, and (iv) that in all the circumstances, the court ought to exercise its discretion to permit service of the proceedings out of the jurisdiction.
CPR PD 6B	3.1. The claimant may serve a claim form out of the jurisdiction (...): (9) A claim is made in tort where - (a) damage was sustained within the

	jurisdiction; or (b) the damage sustained resulted from an act committed within the jurisdiction...

More specifically, the judge decided:

- that misuse of private information was a tort for the purposes of the rules governing service out of the jurisdiction;
- that "damage" under 3.1.(9) meant damage that was recoverable for the tort in question, including damages for distress, recoverable from a claim for misuse of private information (3.1.(9)(a));
- in any case, if 3.1.(9)(a) would not apply, 3.1.(9)(b) would have applied, because *"the damage resulted from an act committed within the jurisdiction, namely the publication of the advertisements on the claimants' screens*".
- that the claimants had established that there were serious issues to be tried as to whether the relevant information was private information;
- that the defendants had a real and substantial cause in their case for misuse of private information under the Data Protection Act ('DP Act').

Google challenged this decision, arguing that:

- misuse of information is not a tort, according to binding authority (*Douglas v Hello No. 3*), and that the meaning of damage in the DP Act was wrongfully applied, also according to binding authority (*Johnson v Medical Defence Union*);
- that there was no serious issue to be tried in relation to any of the claims, because BGI are not personal data and;
- there is not a real and substantial cause of action in relation to the claims for misuse of private information.

The Court of Appeal decided on all these matters. The most important findings:

(i) Whether misuse of private information is a tort

- "The problem the courts have had to grapple with during this period has been how to afford appropriate protection to "privacy rights" under Article 8 of the Convention in the absence of a common law tort of invasion of privacy" (§ 18), "shoe-horning" breach of privacy into breach of confidence (§ 42).
- "Actions for breach of confidence and actions for misuse of private information rest on different legal foundations. (...) they protect different interests: secret of confidential information on one hand and privacy on the other" (§ 25).
- "We do not need to attempt to define a tort here. But if one puts aside the circumstances of its "birth", there is nothing in the nature of the claim itself to suggest that the more natural classification of it as a tort is wrong" (§ 43).
- "We have concluded (...) that misuse of private information should now be recognised as a tort for the purposes of service out of the jurisdiction. This does not create a new cause of action. In our view, it simply gives the correct legal label to one that already exists. We are conscious of the fact that there may be broader implications from our conclusions, for example as to remedies, limitation and vicarious liability, but these

were not the subject of our submissions, and such points will need to be considered as and when they arise" (§ 51).

(ii) The meaning of "damage" in section 13 of the Data Protection Act, in particular, whether there can be a claim for compensation without pecuniary loss

Reference texts

UK DP Act. Section 13	Directive 95/46/EC, Article 23
"(1) An individual who suffers damage by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that damage. (2) An individual who suffers distress by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that distress if— (a) the individual also suffers damage by reason of the contravention, or *(b) the contravention relates to the processing of personal data for the special purposes". (journalism, artistic and literary purposes)*	"1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered."

- The Court first establishes that the situation of the claimants does not fall in any of the two conditions necessary for them to be awarded compensation for non-pecuniary damage, according to the DP Act.
- Acknowledging that the DP Act is transposing Directive 95/46/EC, the Court further analyses whether "damage in Article 23 of the Directive includes non-pecuniary loss" and decides that "*Since what the Directive purports to protect is privacy rather than economic rights, it would be strange if the Directive could not compensate those individuals whose data privacy had been invaded by a data controller so as to cause them emotional distress (but not pecuniary damage). It is the distressing invasion of privacy which must be taken to be the primary form of damage (commonly referred to in the European context as "moral damage") and the data subject should have an effective remedy in respect of that damage.*" (§ 77)
- The Court finds that the conditions under Article 13(2) of the DP Act are too restrictive and it "cannot interpret section 13(2) [of the DP Act] compatibly with Article 23 [of the Directive]" (para 94), which leads to the fact that the Court cannot apply the *Marleasing* doctrine (i.e. consistent interpretation). It further finds that "What is required in order to make section 13(2) compatible with EU law is the disapplication of section 13(2), no more and no less" (§ 105).
- Grounding its decision on Articles 7, 8 and 47 (right to an effective remedy and to a fair trial) of the Charter of Fundamental Rights of the EU, the Court decides to simply disapply Article 13(2) of the national law, which means that "*compensation would be recoverable under section 13(1) for any damage suffered as a result of a*

contravention by a data controller of any of the requirements of the Data Protection Act" (§ 105).

(iii) Whether there is a serious issue to be tried that the BGI is personal data under the DP Act (note - these reasoning could be very important for data protection in Big Data)

- The fact that BGI constitutes personal data "is supported by the terms of the Directive, as explained in the Working Party's Opinion, and the decision of the ECJ in *Lindqvist*. ... If section 1 of the DP Act is appropriately defined in line with the provisions and aims of the Directive, identification for the purposes of data protection is about data that 'individuates' the individual, in the sense that they are singled out and distinguished from all others." (§ 115)
- The Court had regard to the following:
  - "BGI information comprises two relevant elements:

(a) detailed browsing histories comprising a number of elements such as the website visited, and dates and times when websites are visited; and
(b) information derived from use of the 'doubleclick' cookie, which amounts to a unique identifier, enabling the browsing histories to be linked to an individual device/user; and the defendant to recognise when and where the user is online, so advertisements can be targeted at them, based on an analysis of their browsing history" (§ 115).

  - Taking those two elements together, the BGI enables Google to single out users because it tells Google:

(i) the unique ISP address of the device the user is using i.e. a virtual postal address;
(ii) what websites the user is visiting;
(iii) when the user is visiting them;
(iv) and, if geo location is possible, the location of the user when they are visiting the website;
(v) the browser's complete browsing history;
(vi) when the user is online undertaking browser activities. The defendant therefore not only knows the user's (virtual) address; it knows when the user is at his or her (virtual) home (para 115).

  - "The best proof of this is defendant's own business model which is predicated on the potential for the "individuation" of users" (§ 119).
  - "On a straightforward and literal construction of the section (note - article in UK DP Act establishing the definition of personal data), therefore, the fact that a data controller might not aggregate the relevant information in practice is immaterial. What matters is whether the defendant has "other information" actually within its possession which it could use to identify the subject of the BGI, regardless of whether it does so or not." (§ 124).

The Court rejected the Appeal but its decision can be challenged. In the meantime, Google has applied to the Supreme Court to appeal against the Court of Appeal's judgment. On 28 July 2015, the Supreme Court granted Google leave to appeal on certain issues bit it refused to grant it leave to appeal on the ground whether the Court of Appeal was right to hold that claims for misuse of private information were claims made in tort. Leave to appeal on this ground was refused because it did not raise an arguable point of law. See Supreme Court Press Release.

2) Case 15/57/C, *Belgian Commission for the Protection of Privacy v. Facebook Inc., Facebook Belgium SPRL and Facebook Ireland Limited*, 9 November 2015 (Brussels Court of first instance, temporary measures) - unique identifiers cookies placed on non-registered users' browsers

Link

Facts of the case

Facebook offers social plug-ins that website owners can include on their website to enable their visitors to "like" the website's content, to react to it, or share it. When an internet user consults a website on which social plug-ins are included, the browser sends a request to the Facebook server which includes the IP address, the URL of the website, the operating system of the browser, the type of browser and the cookies previously placed on the browser by the Facebook server.

Facebook places a cookie containing a unique browser identifier ("datr cookie") in the browser of internet users visiting a website of the facebook.com domain, whether they are registered user or not. This cookie is retained on the users' computer for a period of 2 years. Facebook Ireland keeps access logs containing anonymous datr cookie identifiers and IP address details. As a result, Facebook can monitor their surfing behaviour of internet users through a combination of the datr cookies, the IP address and the website that they visited.

The Privacy Commission issued a Recommendation stressing that the processing of personal data about non-registered users by means of cookies and social plug-ins does not comply with Belgian privacy legislation and ordering Facebook to refrain from systematically placing long-life and unique identifier cookies with non-registered users. Following a failure to comply with the order, the Privacy Commission brought proceedings to order Facebook to cease (1) placing a datr cookie on non-registered users' browsers without their consent and (2) collecting the cookie on third-party websites through social plug-ins.

Main findings of the Court

1) Admissibility: Belgian law is applicable based on Art. 4(1)(a) of Directive 95/46

- The Court recalled that Directive 95/46 is applicable regardless of whether the processing takes place within the European Union because it applies under Art. 4(1)(a) where the processing is carried out in the context of the activities of an establishment of the controller on the territory of a Member State. (pp.12-13)
- The Court held that the activities of the controller[6] and those of Facebook Belgium are ***''inextricably linked''*** in the meaning of *Google Spain* because Facebook Belgium's main activities include sales support and marketing services. (pp.13-15)
- The Court explained that *"**processing of personal data** to the benefit of a service of a social network site such as Facebook, which is operated by an enterprise with its Registered Office in a third country but an establishment in a Member State, **is carried out ''in the context of the activities'' of this establishment if the establishment is intended to ensure the promotion and sale in that Member State of***

[6] The Brussels Court of First Instance held that it is irrelevant whether the controller is Facebook Inc or Facebook Ireland whereas Facebook contends that the controller is Facebook Ireland.

advertising space offered by this social network site, which is intended to make the service offered by this social network profitable''.

- The Court stated that the display of personal data on a Facebook page constitutes processing of such data. Accordingly, this processing is *"carried out in the context of the advertising and commercial activity of the establishment of the controller on the territory of a Member State*" because the Facebook page also includes advertising related to the activities of the user.
- It added that ***''ensuring relations with the public administration and lobbying activities''*** is also intended to make the social network profitable and is inextricably linked to the activities of the Facebook Group. (p.15)

2) Substance

Processing of personal data (pp.22-23)

- The Court found that a datr cookie constitutes personal data because it contains a unique identifier and it is used in part to decide who should be granted access to a Facebook service.
- Moreover, it recalled that the CJEU in case C-70/10 *SABAM* and the Art.29 WP have already confirmed that IP addresses constitute personal data.
- It concluded that the **''*automated processing of IP addresses and uniquely identifying browser cookies*'' must be considered as processing of personal data** and must comply with the relevant obligations.
- This also concerns "*the simple storage or the simple automated reception of this data from the browser of a user visiting a website with a social plug-in''*.

Consent (pp.23-26)

- The Court held that the unambiguous consent of the data subject cannot be used as a legal basis for placing a datr cookie in the case of non-registered users who visited a page of the facebook.com domain.
- Belgian law specifies that "*the storage of information or obtaining access to information already stored in the end user's final equipment''* is only authorised if the data subject has granted consent after receiving *''clear and precise information about the purposes of the processing and his rights*" except in the case of storage or access for technical purposes.
- The Court quoted the Irish DPA which stated that *''cookies essential to delivering the service requested by the user*" do not require consent and that *''this will generally be the case where the cookie is stored only for as long as the ''session'' is live and will be deleted at the end of the session''*. However, this was not the case because the datr cookie is not deleted and is kept for two years.
- When an internet user visits a facebook.com website for the first time, Facebook shows a cookie banner warning about their use of cookie and provides a link to the cookie policy. The datr cookie is placed if the user clicks on hyperlinks on the cookie policy page such as 'Facebook services'. The Court held that this does not constitute informed consent because the user is still gathering information at this stage.
- When an internet user visits a website with a social plug-in, the cookie is not placed if the user clicks on the plug-in but it is placed if the user decides to cancel and close the plug-in. The Court held that this does not constitute informed consent because the user specifically indicates that he does not want to use the service.

- The Court found that Facebook does not have the consent of the data subject to read the cookie previously placed on the browser either because Belgian law requires consent both to place the cookie and to gain access to it.
- While a registered user may implicitly and unambiguously consent to the placing and reading of the datr cookie by accepting the terms and conditions, this does not hold true for non-registered users who visit a page of the facebook.com domain.
- The Court concluded that ***''since the personal data of non-registered users, especially in case of ill-considered use of the banner or of the social plug-in, can already be processed before this non-registered user is able to obtain complete information or does not even wish to use the social plug-in or more generally the Facebook services, this data is seemingly not processed fairly and lawfully, and it is not obtained for specified, explicit and legitimate purposes or it is further processed in a way which, taking into account all the relevant factors, i.e. the reasonable expectations of the data subject and the applicable statutory and regulatory provisions, is incompatible with those purposes''***.

Performance of a contract (p.26)

- The Court held that there is no agreement between a non-registered user and Facebook and he/she did not give a valid consent to the terms of use therefore the processing is not necessary for the performance of a contract or prior to it.

Compliance with a legal obligation (pp.26-27)

- The Court recalled that the data security obligations cannot be used as a ground to legitimise processing.

Legitimate interests (pp.28-29)

- The Court rejected the argument according to which accessing the datr cookie when a non-registered user visits a website with a social plug-in is *''necessary to ensure the security of Facebook services*''. Even if it were the case, the Court found that less intrusive methods seem to exist.
- *''Collecting the personal data of non-users of Facebook through social plug-ins undeniably makes it possible to expose and record a significant part of the surfing behaviour of non-users of Facebook, taking into account the large number of websites with a Facebook social plug-in. Consequently, this has a* ***serious impact on the fundamental right to privacy and the protection of personal data****, and it must also be observed, moreover, that Facebook, as a large Internet group, is in a much* ***stronger position*** *than the individual non-user of Facebook''.*
- The **interests of non-registered users prevail because the processing is ''*** ***clearly disproportionate considering the indicated purpose and the scale on which the processing operations are carried out and that that these are not fair or legitimate processing operations either''***.

Other grounds (p.28)

- The processing is not necessary to safeguard a vital interest of non-registered users nor is it carried out in the public interest or in the exercise of an official authority.

3) Proportionality of the measures (p.30)

- The violations breach the fundamental right of a very large group of persons, there are millions of websites with Facebook social plug-ins and often sensitive information is at stake.
- Moreover, violations of the principles relating to data quality and the criteria for making data processing legitimate are a matter of Belgian public order.
- It is irrelevant that the technical implementation to comply with the order needs to take place abroad because of the way that the company is structured.

Conclusion (p.32): The Court ordered Facebook Inc, Facebook Belgium Sprl and Facebook Ireland Limited in respect of non-registered users to cease:
"1) *placing a datr cookie when they land on a web page of the facebook.com domain without providing them with prior sufficient and adequate information about the fact that Facebook places the datr cookie with them and about the way Facebook uses that datr cookie through social plug-ins*;
2) *collecting the datr cookie through social plug-ins placed on third-party websites.*"

The Court also imposed a fine of EUR 250 000 for each day that the order is not complied with.

IV. PENDING CASES

COURT OF JUSTICE OF THE EUROPEAN UNION

1) Request for a preliminary ruling from the Bundesgerichtshof (Germany) lodged on 17 December 2014 in Case C-582/11 *Patrick Breyer v Bundesrepublik Deutschland* – collection of IP addresses for the functioning of a telemedium under Art. 7(f) of the Directive 95/46

Link

Questions referred:

(1) Must Article 2(a) of Directive 95/45 be interpreted as meaning that an IP address which a service provider stores when his website is accessed already constitutes personal data for the service provider if a third party (an access provider) has the additional knowledge required in order to identify the data subject?

(2) Does Article 7(f) of Directive 95/45 preclude a provision in national law under which a service provider may collect and use a user's personal data without his consent only to the extent necessary in order to facilitate, and charge for, the specific use of the telemedium by the user concerned, and under which the purpose of ensuring the general operability of the telemedium cannot justify use of the data beyond the end of the particular use of the telemedium?

2) Request for a preliminary ruling from the Raad van State (Netherlands) lodged on 24 April 2015 in Case C-192/15 *Rease and Wullems* - notion of 'making use of equipment' and scope of powers of the DPA in Directive 95/46/EC

Link

Questions referred:

(1) Does an instruction to employ equipment for the processing of personal data within the territory of a Member State, issued outside the EU by a controller, within the meaning of Article 2(d) of Directive 95/46/EC, to a detective agency established within the EU, come within the notion of 'making use of equipment' within the meaning of Article 4(1)(c) of that directive?

(2) Does Directive 95/46/EC, in particular Article 28(3) and (4) thereof, given the objective of that directive, allow the national authorities the latitude, when enforcing the protection of individuals by the supervisory authorities provided for in that directive, to set priorities which result in such enforcement not taking place in the case where only an individual or a small group of persons submits a complaint alleging a breach of that directive?

3) Request for a preliminary ruling from the Oberster Gerichtshof (Austria) lodged on 27 April 2015 in Case C-191/15 *Verein für Konsumenteninformation v Amazon EU Sàrl* – applicable data protection law where contracts are concluded in the course of electronic commerce with consumers residing in other Member States

Link

Questions referred relating to data protection:

Is the processing of personal data by an undertaking that in the course of electronic commerce concludes contracts with consumers resident in other Member States, in accordance with Article 4(1)(a) of Directive 95/46/EC, and regardless of the law that otherwise applies, governed exclusively by the law of the Member State in which the establishment of the undertaking is situated in whose framework the processing takes place or must the undertaking also comply with the data protection rules of those Member States to which its commercial activities are directed?

4) Request for a preliminary ruling from the Kammarrätten i Stockholm (Sweden) lodged on 4 May 2015 in Case C-203/15 *Tele2 Sverige AB* v *Post- och telestyrelsen* - compatibility of the retention of traffic data with the ePrivacy Directive and the Charter (AC)[7]

Link

Questions referred:

(1) Is a general obligation to retain traffic data covering all persons, all means of electronic communication and all traffic data without any distinctions, limitations or exceptions for the purpose of combating crime compatible with Article 15(1) of Directive 2002/58/EC, taking account of Articles 7, 8 and 15(1) of the Charter?

(2) If the answer to question 1 is in the negative, may the retention nevertheless be permitted where:

(i) access by the national authorities to the retained data is determined as described in this request for a preliminary ruling, and

(ii) security requirements are regulated as described in the present request, and

(iii) all relevant data are to be retained for six months, calculated as from the day the communication is ended, and subsequently deleted as described in the present request?

[7] Please note that the case will be heard on 12 April 2016 together with C-698/15 Davis (see below).

5) Request for a preliminary ruling from the Corte Suprema di Cassazione (Italy) lodged on 23 July 2015 in Case C-398/15 *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni* - right to erasure - limits on the disclosure of personal data through commercial registers.

Link

The applicant in the main proceedings is an entrepreneur who was declared bankrupt in 1992. This information is still available in a public register and this causes harm to his business.
The Italian Corte di Cassazione asks whether Directive 95/46 (Art 6 (e), in particular) implies a time limit for publications of personal data in a public register. Information normally remains forever in these types of registers, accessible to everyone, as also required under EU law (Directive 68/151).
The second question asks whether Directive 68/151 allows any limitations to publication.

Questions referred:

(1) Must the principle of keeping personal data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed, laid down in Article 6(e) of Directive 95/46/EC, preclude disclosure by means of the commercial registers provided for by the First Council Directive 68/151/EC of 9 March 1968 and by some national law provisions, in so far as it requires that anyone may, at any time, obtain the data relating to individuals in those registers?

(2) Accordingly, may it be considered as permissible under Article 3 of the Directive 68/151/EC for the data be available only for a limited period and only to certain recipients, on the basis of an assessment case by case by the data manager?

6) Request for a preliminary ruling from the Tribunal Supremo (Spain) lodged on 31 July 2015 in Case C-424/15 *Xabier Ormaetxea Garai and Bernardo Lorenzo Almendros v Administración del Estado* - similarities between the conditions of independence of national regulatory authorities for electronic communications and the national data protection supervisory authorities

Link

Questions referred relating to data protection:

(1) Must the conditions of 'independence' of national regulatory authorities for electronic communications networks and services, referred to in Article 3(2) and (3a) of Directive 2002/21/EC, as amended by Directive 2009/140/EC, be the same as those required for national supervisory authorities for data protection under Article 28 of Directive 95/46/EC?

(2) Is the decision in the judgment in *Commission* v *Hungary*, C-288/12, applicable to a situation in which the officers of a national telecommunications regulatory authority are dismissed before their term of office has expired owing to the requirements of the new legal framework which creates a supervisory body grouping together various national regulatory authorities for regulated sectors?

7) Request for a preliminary ruling from the Court of Appeal (United Kingdom) lodged on 28 December 2015 in Case C-698/15 *Davis and others* - extent to which Member States can impose national data retention obligations in light of *Digital Rights Ireland*[8]

Link (information not yet available)/ Link (decision to refer)

Facts of the case

In 2014, the United Kingdom enacted the Data Retention and Investigatory Powers Act (DRIPA) following the invalidation of the Data Retention Directive by the CJEU in *Digital Rights Ireland*. The legality of DRIPA was challenged in front of the Divisional Court which held that the data retention provisions of DRIPA were not compatible with Articles 7 and 8 of the Charter.

The Court of Appeal is currently hearing the appeal of this decision and decided to refer questions to the CJEU concerning the effects of *Digital Rights Ireland*. Although its provisional view differs from the decision of the Divisional Court, it noted that courts in Austria, Slovenia, Belgium, Romania, the Netherlands and Slovakia invalided national legislation applying *Digital Rights Ireland*.

DRIPA will expire on 31 December 2016 and the Court of Appeal asked to examine this request together with the pending preliminary ruling request from the Stockholm Administrative Court of Appeals in Case C-203/15 *Tele2 Sverige AB*.

Questions referred:

(1) Did the CJEU in *Digital Rights Ireland* intend to lay down mandatory requirements of EU law with which the national legislation of Member States must comply?

(2) Did the CJEU in *Digital Rights Ireland* intend to expand the effect of Articles 7 and/or 8, EU Charter beyond the effect of Article 8 ECHR as established in the jurisprudence of the ECtHR?

EUROPEAN COURT OF HUMAN RIGHTS

1) Case n°35252/08, *Centrum För Rättvisa v. Sweden*, communicated on 14 October 2014 - alleged violation of Article 8 by state practice and legislation concerning secret surveillance and lack of effective domestic remedy

Link

Centrum För Rättvisa, a Swedish non-profit public interest law firm, complains that Swedish state practice and legislation concerning secret surveillance measures violate Article 8 and that there is no effective domestic remedy. The applicant alleges that prior to the entry into force of the FRA Act authorising the Swedish National Defence Radio Establishment (FRA) to carry out surveillance on wireless and wired communications, FRA conducted unregulated surveillance. Moreover, the applicant affirms that the FRA Act is not compatible with the Convention. Despite the minimum standards developed by the Court to avoid abuses of

[8] Please note that the case will be heard on 12 April 2016 together with C-203/15 Tele2 (see above).

power, the Act contains only one of the safeguards, namely, the duration of an interception. The applicant also argues that certain supervisory powers do not constitute effective remedies. Finally, the Centrum För Rättvisa explains that the claim is admissible because the mere existence of legislation which allows a system for the secret monitoring of communications entails a risk of surveillance to all those to whom the legislation may be applied, regardless of whether measures were actually taken.

2) Case n°58170/13, *Big Brother Watch v. United Kingdom*, communicated on 7 January 2014 - alleged violation of Article 8 following surveillance by GCHQ through its own programme and through information received from the United States

Link

The applicants complain that they are likely to have been the subject of general surveillance by GCHQ and/or that the United Kingdom security services may have received material intercepted by the United States relating to their electronic communications in violation of Article 8 of the Convention. They allege that the interferences are not in accordance with the law, and even if they were, the interference would be inherently disproportionate.

According to the applicants, the NSA interception programmes provide very broad access to the content and metadata of non-US persons' communications and allow for this material to be collected, stored and searched using keywords. They refer to PRISM which, according to media reports, allows the NSA to access a wide range of internet communication content and metadata from US corporations. Since a substantial amount of global data passes through the servers of American companies, their emails could possibly have been intercepted. They also refer to a programme called UPSTREAM which provides access to the NSA to nearly all the traffic passing through fibre optic cables owned by US communication service providers.

According to the documents leaked by Edward Snowden, the GCHQ has had access to PRISM material since at least June 2010 and runs a surveillance programme called TEMPORA, which is authorised by certificates issued under section 8(4) of the Regulation of Investigatory Powers Act 2000. The applicants claim that it gives access to electronic traffic, including the content and metadata of internet and telephone communications, passing along fibre-optic cables running between the United Kingdom and the North America. They also allege that the US agencies were given access to the information collected by TEMPORA.

3) Case n°70838/13, *Antović and Mirković v. Montenegro*, communicated on 3 December 2014 - CCTV in auditoriums of universities

Link

The applicants, professors of a University, were informed by the Dean that video surveillance cameras would be installed in the auditoriums for the purpose of safety of property and people, safety of students and surveillance of teaching. Access to the data collected was protected by codes only known by the Dean and stored for a year. The applicants addressed a complaint to the national DPA requesting that the cameras, installed without their consent, would be removed. The DPA held that the reasons for the introduction of video surveillance were not met, given the fact that there was no evidence that safety of people and property was threaten in the auditoriums, even less confidential data, and surveillance of teaching was not

amongst the legitimate grounds for video surveillance. Cameras were removed 9 months later and data erased.
The applicants filed a compensation claim against the University, the State and the DPA. The courts held that the University was a public institution performing activities of public interest (i.e. teaching) and thus video-surveillance in the auditoriums, public places, could not violate their right to private life.
The applicants complain under Article 8 of the Convention that the unlawful installation and use of video surveillance in the auditoriums where they held classes violated their right to privacy.

4) Case n°38940/13, *Buda v. Poland*, communicated on 19 January 2015 - against decision of national court stating that all Internet users are public figures

Link

The applicant was a user of his university forum hosted by a social medical internet portal. Insults and threats were expressed regarding his views on subjects such as abortion, including from the moderator of the forum. The company did not remove the posts.
The Court of Appeal agreed that the company failed in promptly removing the contents indicated by the applicant while it had had knowledge of their existence and nature. But the Court held that no personal right had been infringed. It considered that a person regularly participating in internet discussion forum should be considered a person involved in public life. By expressing his views, he consented to them being assessed by other participants and should expect that some comments might be negative and critical, as long as they did not exceed the limits accepted by the society.
The applicant complains under Article 10 of ECHR about the court finding that users of the Internet are public figures and thus not entitled to protection against insults and threats.

5) Cases n°1874/13 and 8567/13, *Lopez Ribalda v. Spain*, communicated on 17 February 2015 - video surveillance at the work place

Link

An employer installed visible surveillance cameras directed into the entries and exists of the supermarket and hidden ones into the checkout counters to record and control possible thefts committed by the employees. Neither the employees nor the Staff Committee were informed about the existence of these hidden cameras. Two employees were dismissed for theft based on the recordings.
The High Court of Justice of Catalonia confirmed that the dismissals were lawful. In case of covert video surveillance of an employee on suspicion of theft, the employer's fundamental right to respect for his property rights had to be weighed against the employee's fundamental right to privacy.
The applicants complain under Article 6 § 1 and 8 of ECHR that the employer had the obligation to previously inform them about the instalment of hidden surveillance cameras that were directed into their workplace.

6) Case n°62357/14, *Benedik v. Slovenia*, communicated on 8 April 2015 - disclosure of IP address to the police without a court order

Link

Upon request of the police, an internet service provider disclosed the applicant's name, surname and address, his telephone number and the time of the communication. The Courts held that the applicant must have been aware of 630 pornographic pictures and 199 videos involving minors he had downloaded through p2p networks and made available for sharing with other users. He was convicted of child pornography. Moreover, the Courts held that the IP address concerned solely the name of an owner or user of electronic communication, thus the data could be obtained without a court order.
The Constitutional Court dismissed that applicant's appeal. Traffic data, which includes the IP address, is protected by the Constitution. But the applicant had established an open line of communication with an undetermined number of strangers and therefore his expectation of privacy was not legitimate.
The applicant complains under Article 8 of ECHR that his right to privacy was breached because his IP address and consequently his identity were gathered without a court order.

7) Case n°48534/10, *Rodina v. Latvia*, communicated on 12 May 2015 - privacy vs freedom of expression

Link

A newspaper article stated that the applicant had taken her mother to a psychiatrist hospital, sold her mother's apartment and refused to support her. It was accompanied by a photograph of the family showing the applicant, her mother, husband, son, sister and sister's daughter, and the mother's husband. The applicant was contacted by a journalist prior to the publication but she refused to comment and requested that her name was not published. The Regional Court found that the article reflected an opinion and that the photograph was neutral so the publication did not damage the applicant's honour.
The applicant complains under Article 8 that the Court failed to protect her right to respect for her private life.

8) Case n°49108/11, *Samoylova v. Russia*, communicated on 13 May 2015 - unlawful collection of data and use in criminal proceedings

Link

The applicant's husband was a prosecutor charged with a number of criminal offences. A TV programme was released on the trial revealing certain information concerning the applicant (home address, tax-payer identification number, income, estate), as well as a video recording and photographs showing the interior of her residence.
The applicant complains under Article 8 of ECHR about unlawful collection, unlawful and disproportionate disclosure of the following data and information. She also alleges that the State officials directly provided or assisted the journalist in obtaining this information and data.

9) Cases n°78392/14 and 2229/15, *Bileski and Karajanov v. Macedonia*, communicated on 19 May 2015 - unlawful disclosure of personal data by public authority

Link

A holder of public office could be disqualified from the office and prevented to perform any public duty if the Commission on verification of facts establishes that he was registered as "a secret collaborator, operational liaison or secret informant with the State security bodies after 1944. The cooperation should be "intentional, secret, organised and continuous" and it should entail "material benefit or a privilege in employment or career advancement".
The Commission found that the applicants cooperated with the State security bodies and published its decisions on its website with their full name, date and place of birth, single identification number and the public office which they held.
The applicants complain that the authorities refused to consider evidence and examine witnesses, did not provide sufficient reasons for their decisions and that they were given limited access to the relevant documents in violation of Article 6 ECHR. Mr. Bileski also complains under Article 8 that the authorities created, stored and made public information about him without his consent, which had adverse effects on his private and family life, as well as on his reputation and right to perform the office of a judge.

10) Case n°66490/09, *Mockute v. Lithuania*, communicated on 19 June 2015 - confidential health data

Link

The applicant joined a religious group before being taken by her family in a psychiatrist hospital. A TV programme showed an interview with the applicant's psychiatrist. She states that the psychiatrist, without her consent, disclosed information about her studies, personal life and medical history, from which she could be identified. The applicant's mother and sister, as well as her apartment were shown in the programme.
The Court of Appeal did not find any breach of privacy. It referred to a letter addressed to the journalists of the programme acknowledging its initiation by her family members and that she was given another name.
The applicant complains that it was possible to identify her, that the broadcast did not have her prior permission. In addition, the journalists relied on the information provided by the psychiatrist who was treating the applicant, which was against the rule that medical data is confidential.

11) Case n°8630/11, *Suprunenko v. Russia*, communicated on 19 October 2015 - arrest data stored and published in a classified database for an indefinite period of time

Link

The applicant is an advocate doing reportage in his ancestral town. He was arrested for taking picture of a school. At the station, the officers fingerprinted the applicant, took a mugshot, and catalogued his body features. The book entry indicated his name, date and place of birth, ethnic origin, detention status, permanent and temporary addresses, physical data (height, frame, hair, face colour, eye colour, and tattoos), date of arrest, and ID details. The officer told the applicant that this data would be indefinitely held on a database of the Interior Ministry.
The applicant complains under Article 8 ECHR that despite that fact that he did not commit any crime, his personal information is held in a classified database.