

Reference for a preliminary ruling
Fővárosi Törvényszék
(Budapest Municipal Court - Hungary)
lodged on 15 September 2015 —
Juliette Fleurie v. Facepage Hungary

(Case C-296/15)

Language of the case: Hungarian

Referring court

Fővárosi Törvényszék

Parties to the main proceedings

Applicant: Juliette Fleurie

Defendant: Facepage Hungary

Questions referred

1. In a case such as the one at hand, does the fact that a court of a Member State has declined jurisdiction on the grounds of *lis pendens* have a binding effect on a court's ability in another Member State to decide the case?

If question 1) is answered in the negative,

2. does the court of a Member State have to stop the proceedings of a company under Articles 29 and 30 Regulation 1215/2012 when the “mother company” is being sued in another Member State?

If questions 1) and 2) are answered in the negative,

3. for the purpose of the identification of the applicable law under Article 4 Directive 95/46/EC (Data Protection Directive), can a subsidiary to an enterprise that is established in one Member State, that also has a small office in another Member State, be considered as being established in this other Member State, if this office only offers technical support and customer assistance?

If question 3) is answered in the affirmative

4. does a national law that i) *a priori* qualifies any confrontation between a person and the police as triggering the public policy exception to data protection, and ii) provides an exemption from damages' compensation whenever public

policy is concerned, conflict with the Data Protection Directive?

5. may a data controller make exceptions from its general duty to delete data, where the storage and accessibility of the data is supported by reasons of the public information interest under Articles 7 and 8 EU-Charter?

If question 4) is answered in the affirmative and question 5) is answered in the negative,

6. does the Data Protection Directive have direct effect in establishing the liability of the controller of the data and the right to compensation, considering Articles 7 and 8 EU-Charter and Article 8 ECHR?

Reference for a preliminary ruling
from the Cour de Cassation, France
lodged on 16 September 2015 —
Sandrine Bonnaire v Huxiyun Ltd

(Case C-297/15)

Language of the case: French

Referring court

Cour de Cassation, France

Parties to the main proceedings

Applicants: Sandrine Bonnaire,

Nicolas Duvauchelle

Defendant: Huxiyun Ltd

Questions referred

1. Taking into account that Huxiyun Ltd is a Japanese enterprise, does a policy of measuring the basic pay in individual salary groups by age categories and gender categories, infringe the primary-law prohibition of age discrimination and gender discrimination (now Article 21(1) of the CFREU) as given expression by Directive 2000/78/EC?
2. Taking into account the right of parties to a collective agreement to collective bargaining which is guaranteed by primary

All information given on the case and on the content of the Hungarian law is fictitious and should be relied on for the purpose of the Moot.

Background:

Juliette Fleurie, a French national that is resident in France, is spending her holidays travelling through Europe during February 2015.

After having visited Cambridge, Genoa, Valencia, Leuven, Münster, Hamburg, Katowice and Wrocław, she finally goes to Hungary. While staying in Budapest, she wants to share the pictures of the last leg of the journey with the friends that she met during her trip. She decides to create a Facepage account from the computer of the hotel and uploads the pictures she took in Budapest. She is asked to give her consent to several things and, without paying much attention, just ticks the “yes” box several times. Thereby, she also accepts that “friends” have “full access to all pictures she uploads”.

On the last day of her stay, some Hungarian friends, amongst which there is the well-known Hungarian activist László Nagy, persuade her to take part in a protest march, and she accepts. Unfortunately, the protest march turns out to be disorderly and some tensions occur between the demonstrators and the police.

During the march, a friend of Juliette takes pictures, showing them participating in the protest in general and also in direct conflicts with the police. The evening of the same day, Juliette uploads the photos on her Facepage profile. László Nagy who is very proud of Juliette’s involvement in the march downloads the pictures from her account and, later uploads them to his own Facepage profile. He puts Juliette’s name in the text under the profile. The Facepage software recognises the image of Juliette and automatically links the picture to her profile.

The following morning, however, Juliette changes her mind and deletes the photos of her participating in the march. She even closes her Facepage account altogether, not worrying about what will happen to pictures of her uploaded in other persons’ profiles. Then she leaves Budapest, going back home to France.

On March 2015, Juliette starts to look for a new job in the Public Administration sector in Paris. Three months later, a PA to which she made an application, is investigating upon her in order to proceed with the enrolment.

Doing some research on the applicants on the web, the PA finds the photos of Juliette participating in the march in Budapest and being involved in the conflicts with the Hungarian police. He decides not to consider her because of her conduct and her social profile. It was easy to find the photos, although they had been deleted from Juliette’s page, since they were still linked to her name on Facepage.

After receiving a letter that explains why she was not enrolled on May the 4th 2015, Juliette sues Facepage International before the Tribunal de Paris for the damages caused by the record of the pictures. Unfortunately, just a few days later, a law comes into force in the US which strictly limits the enforceability of data protection titles in the US. Juliette’s lawyer immediately suggests not putting too much hope into the case in France and instead suing the EU partner companies of Facepage.

Therefore, Juliette sues Facepage Ireland before an Irish Court for the compensation of the damages caused by the record of the pictures. The Irish court dismisses the claim on the grounds of *lis pendens*. It considers the Facepage companies as one entity.

Then, on July the 10th, she brings an action before the Fővárosi Törvényszék (Budapest Municipal Court) against Facepage Hungary for the compensation of the damages she suffered from not being employed by the PA.

Facepage International is a company having its seat in the US and which has many daughter companies worldwide in order to manage the local provision of services

Facepage Ireland is a company having its seat in Ireland, but which is fully controlled by Facepage International. It provides expert services throughout Europe. It is the local service provider for Europe and manages all European accounts following the directives given by the mother company.

Facepage Hungary is a partner company to Facepage Int. and Facepage Ireland. Facepage Hungary has a small office in Budapest with one permanent position and regular visits by employees from Facepage Ireland. Facepage Hungary is only responsible for technical support, such as the use of the facial recognition software, and for customers' assistance.

In the structure of the company, Facepage Ireland may be understood as a daughter of Facepage Int., while Facepage Hungary would be a daughter of Facepage Ireland.

The case before the Hungarian Court:

Juliette Fleurie asks the Court not to stop the proceedings on the grounds of *lis pendens*.

On the merits, she finds Facepage Hungary liable for not removing the pictures from the platform. At least, Facepage should be held responsible for linking her name to the photos.

She asks for the application of Irish instead of Hungarian Law, as Irish law is the law of establishment of Facepage Ireland, which in its turn is the company that controls Facepage Hungary.

In case this is denied, she asks for the direct application of the Directive since national law (Hungary) has not properly implemented the Directive and, therefore, does not protect the personal data of internet users sufficiently and neither grants a proper compensation of damages.

Facepage Hungary challenges the jurisdiction of the Hungarian court considering the binding effect of the Irish decision (ECJ Gothaer C-456/11).

On the merits, Facepage Hungary states that there is no liability at all.

Firstly, Facepage Hungary asks for the application of Hungarian law.

In order to avoid the responsibility and the obligation to pay compensation of damages, Facepage Hungary brings forward the following arguments:

- a) There is valid consent by Juliette Fleurie to the policy rules set by Facepage when she created her account.
- b) There is no liability under article 23.2 Data Protection Directive because the pictures were uploaded by third parties.
- c) Hungarian Law, in this case, obliges data controllers to keep and store personal data.
- d) Under Hungarian law, there also is an exemption from the duty to compensate damages for public policy reasons.
- e) In any case, under the ECJ Google Spain decision (C-131/12), a data controller must make exceptions from deleting the data where the storage and accessibility of the data is supported by public information interests that justify the interference with the customer's fundamental rights.

Relevant Provisions

REGULATION (EU) No 1215/2012 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters(recast)

Article 29

1. Without prejudice to Article 31(2), where proceedings involving the same cause of action and between the same parties are brought in the courts of different Member States, any court other than the court first seised shall of its own motion stay its proceedings until such time as the jurisdiction of the court first seised is established.
2. In cases referred to in paragraph 1, upon request by a court seised of the dispute, any other court seised shall without delay inform the former court of the date when it was seised in accordance with Article 32.
3. Where the jurisdiction of the court first seised is established, any court other than the court first seised shall decline jurisdiction in favour of that court.

Article 30

1. Where related actions are pending in the courts of different Member States, any court other than the court first seised may stay its proceedings.
2. Where the action in the court first seised is pending at first instance, any other court may also, on the application of one of the parties, decline jurisdiction if the court first seised has jurisdiction over the actions in question and its law permits the consolidation thereof.
3. For the purposes of this Article, actions are deemed to be related where they are so closely connected that it is expedient to hear and determine them together to avoid the risk of irreconcilable judgments resulting from separate proceedings.

ECHR

Article 8 - Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Article 14 - Prohibition of discrimination

The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.

CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION

Article 7 - Respect for private and family life

Everyone has the right to respect for his or her private and family life, home and communications.

Article 8 - Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

EUROPEAN CONVENTION OF HUMAN RIGHTS

Article 8 - Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Article 14 - Prohibition of discrimination

The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status

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

Article 4 National law applicable

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:
 - (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;
 - (b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;
 - (c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.
2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

Article 7

Member States shall provide that personal data may be processed only if:

- (a) the data subject has unambiguously given his consent; or
- (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
- (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
- (d) processing is necessary in order to protect the vital interests of the data subject; or
- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
- (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

Article 13

Exemptions and restrictions

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measure to safeguard:

- (a) national security;
- (b) defence;
- (c) public security;
- (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
- (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
- (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
- (g) the protection of the data subject or of the rights and freedoms of others.

2. Subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual, Member States may, where there is clearly no risk of breaching the privacy of the data subject, restrict by a legislative measure the rights provided for in Article 12 when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.

Article 23 Liability

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.

2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

Hungarian Law

Law on electronic communications (transposing the Directive on Data Protection)

[...]

PART III - REQUIREMENTS AND CRITERIA FOR PROCESSING

Requirements for processing.

Art. 7. The controller shall ensure that:

- (a) personal data is processed fairly and lawfully;
- (b) personal data is always processed in accordance with good practice;
- (c) personal data is only collected for specific, explicitly stated and legitimate purposes;
- (d) personal data is not processed for any purpose that is incompatible with that for which the information is collected;
- (e) personal data that is processed is adequate and relevant in relation to the purposes of the processing;
- (f) no more personal data is processed than is necessary having regard to the purposes of the processing;
- (g) personal data that is processed is correct and, if necessary, up to date;

(h) all reasonable measures are taken to complete, correct, block or erase data to the extent that such data is incomplete or incorrect, having regard to the purposes for which they are processed;
(i) personal data is not kept for a period longer than is necessary, having regard to the purposes for which they are processed.

[...]

Criteria for processing.

Art. 9. Personal data may be processed only if:

(a) the data subject has unambiguously given his consent; or

(b) processing is necessary for compliance with a legal obligation to which the controller is subject; to this purpose, the State can rely on other national laws.

[...]

Art. 15 The controller shall be liable at the request of the data subject to immediately rectify, block or erase such personal data that has not been processed in accordance with this Act or with regulations made under this Act.

[...]

PART VI - EXEMPTIONS, RESTRICTIONS AND OTHER MEASURES

Art. 29 - Damages not to be recovered

Despite the right to compensation standing upon any person whose personal data are violated, the controller is exempted from compensation when the data spread is justified by public policy reasons.

This rule has to be interpreted in compliance with article 9 as well as other national laws.

Hungarian Law on the Safeguard of National Public Order

Art. 1 - Scope of application

The provisions of this law shall apply to any company that is established or operating within the Hungarian State

Art. 6 - Criminal Action

Data controllers are obliged to store personal data even without the consent of the person in question if such data concerns public policy, including criminal actions or any confrontation with the public authorities.