Legal Policy & Pandemics
The Journal of the Global Pandemic Network – LPPJ
2021, Vol. 1, Issue 1-2-3, pp. 197-224
DOI 10.53136/9791259994435116

SECTION II – LITIGATION

Case Law Survey on Data Protection – Covid-19 Litigation Project

Chiara Angiolini

Abstract. The article aims at analyzing the data protection case law collected within the COVID-19 Litigation project until November 2021. In particular, the survey focuses on litigation concerning cases where the processing of personal data is directly aimed at addressing the ongoing pandemic. The article firstly provides a very brief overview of the cases, focusing on the purposes of processing (Section 2). Then, the decisions are described in relation to the legal issues they address: the grounds for the processing of public interest and consent (Section 3), the different aspects of personal data processing that have been considered by the Court (Section 4), data transfers outside external borders (Section 5), and the remedies that courts have granted in individual cases, building a classification of those remedies (Section 6). In the course of the analysis, as well as in Section 7, case law trends are critically considered, also looking at future litigation and possible lines of research to be further developed.

Keywords: *Data Protection, Judicial Dialogue, COVID-19, Pandemic, Litigation, Personal Data, Proportionality, Case Law, Privacy*

1. Introduction

The Covid-19 pandemic has led to a twofold increase in the use of digital instruments: on the one hand, technologies are used as a means of coping with the pandemic (*e.g.*,for contact tracing purposes) and, on the other hand, to carry out various daily activities remotely (*e.g.*, education and work). The widespread use of digital technologies during the current crisis has brought with it massive processing of personal data and therefore is likely to generate litigation. The existing case law reflects, at least in part, the two directions outlined: on the one hand, cases concern data processing related to the use of digital tools for performing activities during the pandemic (*e.g.*, e-proctoring systems in the field of education[1]). On the other hand, litigation relates to the processing of personal data which is directly aimed at addressing the ongoing pandemic (*e.g.*, the use of drones for ensuring law enforcement of emergency measures).

This article focuses on the second group of cases, highlighting that within data protection case law, as in other areas, crucial issues concern the balancing of different interests, often protected in the form of fundamental rights, and remedies. The table attached to this article, where each case taken into consideration is briefly described, shows that data protection litigation concerning data processing for facing the pandemic exists in several countries and across continents.[2] Indeed, institutional variety characterizes the jurisdictions considered with regard to substantive law and its enforcers[3]. All legal systems of the considered case law[4] enacted legislation related to privacy and data protection; in some cases, the normative framework was recently reformed, as in the EU and in Brazil, while in other countries, like in India, its reform is under discussion. Legislation concerning DPAs is an example of the institutional variety in relation to the enforcers[5]. For instance, in the EU, under the

[1] See, as an example, the decision of the Amsterdam Court of first Instance C/13/684665 / KG ZA 20-481 (an unofficial translation in English is available here: <https://gdprhub.eu/index.php?title=Rb._Amsterdam_-_C/13/684665_/_KG_ZA_20-481> accessed 26 June 2021. On this decision, see: Chiara Angiolini and others 'Remote Teaching During the Emergency and Beyond: Four Open Privacy and Data Protection Issues of 'Platformised' Education' (2020) Opinio Juris in Comparatione, 1, 46-72.

[2] The table annexed to this article briefly describes each case and includes the hyperlinks to the decisions when available.

[3] More generally, according to the United Nations database, at the global level, 66% of countries have data protection and privacy legislation, 19 % of States do not have that kind of laws, and 10% of countries have draft legislation. See <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide> accessed 12 June 2021.

[4] See the table annexed to this survey. The table sketches an overview of cases, considering the main issues at stake, the nature of data processed, and of parties in the proceedings.

[5] In the EU legal system, the text GDPR is available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679> accessed 11 June 2021. On the Indian legal framework, see, for a first overview M Deva

General Data Protection Regulation (GDPR), DPAs play an important role, as they have a significant set of advisory, investigative and corrective powers.[6] In the Americas, various approaches exist (*e.g.*, in Brazil and Colombia a DPA was created, in Chile a DPA does not exist, in the U.S. the Federal Trade Commission as a consumer protection authority, acts as a privacy enforcement agency).[7]

The objective of the article is twofold. The first goal is to provide a qualitative analysis of data protection case law which has been collected and selected in the framework of the ongoing 'COVID-19 Litigation Project', conducted by the University of Trento.[8] The article discusses cases collected through November 2021. It identifies recurrent legal issues and the data processing aspects that judges consider in their reasoning, and provides an overview of remedies granted by Courts. However, even if the main purpose of this survey is the analysis of judicial pronouncements, some examples of decisions taken by Data Protection Authorities (DPAs) are considered, as in the field of data protection such authorities are often relevant actors. In accordance with the survey's objectives, only DPA decisions concerning a specific case were analyzed, excluding guidelines, opinions and other documents.

The second objective of the article is to build on the qualitative analysis of the case law in order to identify legal questions that may arise in future litigation and the legal issues that need further investigation by scholars.

The analysis begins in section 2, which provides some methodological and comparative remarks and a brief overview of the case law analyzed. Section 3 considers the legal grounds used for processing data. It focuses on the data subjects' consent and public interest as grounds for processing, examining the role played by the principles of necessity and proportionality in the case law. Section 4 identifies and analyses the aspects of data processing that Courts used in their reasoning and analyses Courts' arguments (*e.g.*, data retention period, means of processing).

Prasad, C Menon Suchithra, 'The Personal Data Protection Bill, 2018: India's regulatory journey towards a comprehensive data protection law' (2020) International Journal of Law and Information Technology, 28, 1. At the date of last revision of this survey, the 25th of October 2021, the proposed reform (Personal data protection bill) is pending (it is possible to accede to the legislative procedure here: <http://loksabhaph.nic.in/Legislation/NewAdvsearch.aspx> accessed 11 June 2021. For a first overview of the Israeli system: Soren Zimmermann, 'The legal Framework of Data Protection in Israel: A European Perspective' (2019) European Data Protection Law Review 2, 246, of the Brazilian legal framework, see: Arye Schreiber 'Right to Privacy and Personal Data Protection in Brazilian Law' in Dário Moura Vicente and Sofia de Vasconcelos Casimiro (eds.) *Data Protection in the Internet* (Springer, 2020) 45; of Colombia: Ana Isabel Gómez-Córdoba and others 'El derecho a la protección de datos personales, tecnologías digitales y pandemia por COVID-19 en Colombia' (2020) Revista de bioética y Derecho, 271 <https://revistes.ub.edu/index.php/RBD/article/view/31830/32129> accessed 1 December 2021 and more generally with regard to Latin America: Inter-American Commission on Human Rights, *Pandemic and Human Rights in the Americas, Resolution 1/2020* <https://www.oas.org/en/iachr/decisions/pdf/Resolution-1-20-en.pdf> accessed 1 December 2021; Luca Belli and Nicolo Zingales, 'Data protection and social emergency in Latin America: COVID-19, a stress test for democracy, innovation, and regulation' (2021) International Data Privacy Law, vol. 11, 1, 1-2 <https://academic.oup.com/idpl/article/11/1/1/6129383> accessed 1 December 2021; WIG Aponte 'Protección de Datos y Transparencia de la Información: Perspectivas para la Regulación Post-Pandemia en una Sociedad Digital desde Algunas Experiencias Latinoamericanas' (2020) Direitos Fundamentais & Justiça - special issue - 69; of the legal system in Montenegro: Nasir Muftic Tahir Herenda, 'Sacrificing Privacy in the Fight Against Pandemics: How Far Is Too Far? Examples from Bosnia and Herzegovina and Montenegro', in *Balkan Yearbook of European and International Law* (Springer 2020).

[6] See art. 58 GDPR.

[7] On the topic: Daniel Alvarez-Valenzuela, 'La protección de datos personales en contextos de pandemia y la constitucionalización del derecho a la autodeterminación informativa' (2020) Revista Chilena de Derecho y Tecnologìa, 1, 1. See, for a comparative overview: Dário Moura Vicente and Sofia de Vasconcelos Casimiro 'Data protection in the Internet', in Katharina Boele-Woelki and others (eds.) *General Reports of the XXth General Congress of the International Academy of Comparative Law* (Springer, 2020) 611. For a comparison between different DPAs in Latin America see: Daniel Ospina-Celis and Juan Carlos Upegui Mejía 'EMNBD y Protección de Datos Personales en Brasil, Chile, Colombia y México: La Experiencia Común' in Vivian Newman Pont, Daniel Ospina-Celis, Juan Carlos Upegui (eds.) 'Festín de datos Empresas y datos personales en América Latina' (Centro de Estudios de Derecho, Justicia y Sociedad, Dejusticia, 2020) 217; with regard to the EU system, see the Chapter, VI 'Independent supervisory authorities' of of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation - GDPR) [2016] OJ L 119, 4.5.2016.

[8] On the structure and the project's aims and methodology, see the opening survey of this section Fabrizio Cafaggi and Paola Iamiceli, 'Global Pandemic and the role of courts'. When the author, mainly for language reasons, could not have direct access to the decisions, she relied only on the case summaries drafted by the project's collaborators. When direct access to the judgment was possible, such case summaries were a helpful tool for developing a comparative analysis.

Section 5 describes the case law concerning data transfers outside external borders, a critical aspect of data protection law. Section 6 gives an overview of remedies granted by Courts and, finally, section 7, building on the previous analysis, provides insights for identifying possible future litigation and related emerging legal issues. The last section provides some concluding remarks.

2. Data Processing to Face the COVID-19 Crisis: the Purposes of Processing and the Nature of Subjects who Process Data

As noted above, the article focuses on cases where the processing of personal data is directly aimed at addressing the ongoing pandemic. Thus, it will not deal with the litigation that has arisen due to the massive use of digital technologies for other purposes (*e.g.*, education). This choice allows for a focus on cases where the pandemic is a central element, as the purposes of processing are directly related to it. The following table summarizes the purposes of data processing related to COVID-19 in the case law analyzed.

PURPOSE	DECISION
Contact tracing purposes	**India,** Central Information Commission*, Saurav Das vs Deptt of Information Technology,* 26 November 2020
	India, The High Court of Orissa, *Cuttack, Ananga Kumar Otta v. Union of India & Ors*, WP (C) No. 12430/2020, decisions of 28 May 2020 and 16 July 2020
	India, High Court of Kerala, *Ramesh Chennithala vs State of Kerala*, 21 August 2020
	Austria, Constitutional Court, V 573/2020, 10 March 2021
	Belgium, Council of State, Decision no. 248.124, 5 August 2020
	Belgium, Council of State, no. 248.108, 3 August 2020
	France, French Constitutional Council decision no. 2020/800, 21 May 2020
	Spain, Asturias High Court of Justice, 10 June 2021
	Switzerland, Administrative Court of Zürich, AN.2020.00012, 3 December 2020
Contact tracing purposes and other purposes related to the spread of COVID-19	**India,** High court of Karnataka, *Anivar A Aravind v. Ministry of Home Affairs, GM PIL WP (C) 7483 of 2020*, 25 January 2021
	Israel, High Court of Justice, 2109/20 *Ben Meir v. Prime Minister,* 26 April 2020
	Israel, High Court of Justice, 6732/20 *Association for Civil Rights in Israel v. Knesset* 1 March 2021
Contact tracing and enforcement of COVID-19 measures	**Norway,** Data Protection Authority, decisions of 15 June and 17 August 2020
Enforcement of provisions taken for facing the COVID-19 crisis	**India,** High Court of Kerala**,** *Balu Gopalakrishnan & Anr. v. State of Kerala & Ors.*, W.P. (C). Temp No. 84, 24 April 2020
	France, Council of State, decision no. 441065, of 26 June 2020
	France, Council of State, dec. no. 440916 of 19 June 2020.
	Montenegro, Constitutional Court of Montenegro, decision U - II 22/20, 23 July 2020
Health and social emergency management, including legislation concerning the COVID-19 certificates	**Poland,** Data Protection Authority, no. DKN.5101.25.2020, 12 November 2020,
	France, Council of State, no. 453505, 6 July 2021
	Spain, Supreme Court, no. 1112, 14 September 2021
	Spain, Supreme Court, no. 1103, 18 August 2021
	Colombia, Constitutional Court, judgement C-150/20, 27 May 2020
Health emergency management and research purposes	**Austria,** Data protection authority, Decision of 15 February 2021
	France, Council of State, dec. decision nn. 440442, 440445; 18 May 20220; Council of State, decision n°446155, 22 December 2020
Information through media	**India**, Madras High Court, *Adv. M. Zainul Abideen vs The Chief Secretary*, W.P.No.7491 of 2020, 22 April 2020
Building official statistics	**Brazil,** Federal Supreme Court ADI 6387 MC-REF decisions of 24 April and 7 May 2020
Healthcare management and other purposes	**France,** Council of State, no. 450163, 12 March 2021
	France, Council of State, no. 44493, 13 October 2020

Not surprisingly, the table shows that case law mainly concerns data processing for purposes of collective and public interest, in particular for i) contact tracing; ii) the enforcement of provisions taken for facing the COVID-19 crisis; and iii) health emergency management.

Moreover, the nature of subjects who process data is a relevant aspect, as the provisions

establishing the institutions that process data and setting its governance may have an impact on applicable data processing rules and on the level of transparency. Within the analysed case law the processing is often conducted by public authorities, but on various occasions private companies are involved in the processing[9]. Moreover, sometimes, data processing is carried out by private parties on the basis of an administrative or legislative decision (*e.g.*, restaurant owners process contact details of clients for contact tracing purposes[10]). As to the parties in the proceedings, often private parties (individuals or collective entities) sought the action and public bodies are the defendants (see also the table annexed to this article). [11]

Adopting a bottom-up approach, the reading and the analysis of the cases lead to identifying four main issues which are addressed in the decisions: i) the legal grounds justifying the processing, also relating to its purpose; ii) the concrete aspects of the processing considered relevant by Courts in their reasoning (*e.g.*, means, retention period); iii) the transfer of personal data across national borders; and iv) the remedies provided by the Courts.

3. When Can Personal Data be Processed During the Pandemic? Data Subjects' Consent and Public Interests Grounds in Courts' Decisions

Defining when data processing may be carried out for the purpose of facing the pandemic is a crucial issue within the analyzed case law, as the way in which lawful data processing's boundaries are set on the one hand identifies the limits to the possibility to use data for facing the pandemic, and, on the other hand, clearly influence the level of protection of data subjects.

Most of the decisions analyzed may be divided in two groups: i) cases where the data processing is justified by public health reasons; and ii) cases where data subject consent is required for processing. However, sometimes consent and public interest are both applied as grounds for the processing, with the aim of balancing the various interests at stake (*e.g.*, the Israeli case law). It should be noted here that there are few cases which have not been included in this paragraph because the decisions do not provide elements concerning the grounds for processing[12], or data processing is based on grounds other than public interests related to the pandemic and consent.[13]

3.1. Data Processing Based on Public Health Reasons: the Role of Necessity and Proportionality Principle

On several occasions, Courts assessed cases where data processing was based on public health reasons. The processing of personal data has often been very useful in dealing with the pandemic, notably for monitoring purposes.[14] At the same time, defining the scope of the processing operations necessary for facing the COVID-19 crisis is crucial to prevent

[9] For example, in the case High Court of Kerala, *Balu Gopalakrishnan & Anr. v. State of Kerala & Ors., W.P. (C). Temp No. 84,* 24 April 2020, the Court assessed the lawfulness of a contract between the Government of Kerala and a USA-based software company, aimed at creating an online data platform for data analysis of medical/ health data in relation to COVID-19. In Europe, a case concerned the lawfulness of an administrative act imposing a duty of private health centers to share negative results of PCR tests with public administration (Austrian data protection authority, Decision of 15 February 2021). Moreover, two cases concern the lawfulness of data transfers to a third country, outside the European Economic Area (French Council of State, 12 March 2021, no. 450163, and 13 October 2020, no., 44493). Another French case concerns the lawfulness of data processing, within a platform of health data for facilitating the use of health data for improving the health emergency management and fostering knowledge about covid-19 (French Council of State, dec. no. 440916 of 19 June 2020). Furthermore, in South America, the Brazilian Federal Supreme Court ADI 6387 MC-REF decisions of 24 April and 7 May 2020 reviewed the constitutionality of provisions that obliged telecommunication Companies to share the list of names, telephone numbers, and addresses of their consumers with Brazilian Institute of Geography and Statistics Foundation, for supporting official statistic during the public health emergency resulting from the COVID-19 pandemic.

[10] As to case law concerning restaurant's owners see: Austrian Constitutional Court, 10 March 2021, V 573/2020 ; Belgian Council of State, Decision n°248.124 of 5 August 2020; with regard to media: Madras High Court, *Adv. M. Zainul Abideen vs The Chief Secretary*, W.P.No.7491 of 2020, 22 April 2020.

[11] For a brief description of each case see the table attached to this article.

[12] *E.g.*, Central Information Commission, *Saurav Das vs Deptt of Information Technology,* 26 November 2020; High Court of Kerala, *Ramesh Chennithala vs State of Kerala*, 21 August 2020; Data Protection Authority, decisions of 15 June and 17 August 2020; on data transfers outside external borders: French Council of State, no. 450163, 12 March 2021 and no. 44493, 13 October 2020; on a data breach: Data Protection Authority, no. DKN.5101.25.2020, 12 November 2020.

[13] *E.g.*, on the freedom of press: Madras High Court, *Adv. M. Zainul Abideen vs The Chief Secretary, W.P.No.7491* of 2020, 22 April 2020.

[14] On this aspect see, for instance, the OECD 'Policy Responses to Coronavirus (COVID-19) Tracking and tracing COVID: Protecting privacy and data while using apps and biometrics', 23 April 2020

the pandemic from becoming an opportunity to justify personal data processing in a way that is detrimental to data subjects' rights and interests. For instance, the risks of widespread surveillance are at stake, for example, as shown in the literature, with regard to the future use of collected data beyond the purpose of facing the actual pandemic[15]. However, the rules for organizing these different interests and their interpretation by Courts vary across continents and countries.

In Europe, EU law provides various legal basis for processing. According to one of them, personal data may be processed if such 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 data controller, and it is authorized by law.[16] Moreover, even sensitive data (including health data) may be processed where it is necessary for reasons of substantial public interest, for the provision of health or social care, or treatment or the management of health or social care systems, provided that certain guarantees (*e.g.*, the processing must be authorized by law) are respected.[17] Accordingly, case law within EU countries often focuses on the necessity of processing for the protection of public health and on the existence of a law authorizing it.[18] Three group of cases may be identified by reason of the nature of the subjects who process data: i) public: personal data processed by public authorities; ii) public-private: personal data discosed by public authorities to the public or shared by private parties to public bodies; and iii) private: personal data processed by private parties.

As to data processed by public bodies, in two decisions the French Council of State assessed the lawfulness of data processing conducted by public authorities through drones for ensuring the enforcement of provisions restricting the freedom of movement for facing the COVID-19 pandemic. In both cases, the Council considered that the processing was legitimate in the light of the COVID-19 crisis, as it is necessary for public safety.[19] Nevertheless, in one of these decisions, the French Council of State affirmed that surveillance conducted through drones that process personal data must stop and may restart only if, after the opinion of the French DPA (*CNIL*), it is approved through a regulatory text authorizing the creation of a personal data processing system in compliance with applicable law.[20] In its reasoning, the Council of State mentioned the principle of proportionality, affirming that the measures taken by public authorities in order to fight the pandemic which may limit the exercise of fundamental rights and freedoms must be necessary, appropriate and proportionate to the objective of safeguarding public health which they pursue.[21]

In another case, the French Council of State, in the light of the current health risks, upheld the necessity and proportionality of health data processing within the French Health Data Hub for purposes of fighting the COVID-19, where the Minister of Health authorized this processing.[22] Moreover, in its decision 2020/800 of 21 May 2020 concerning the processing of health data by public bodies for combatting COVID-19, the French Constitutional Council's reasoning focused on the necessity assessment.[23] In particular, the Council decided on the necessity of data processing for fighting the pandemic, stating that it is justified that a number of public bodies in charge of health

<https://www.oecd.org/coronavirus/policyresponses/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics-8f394636/> accessed 22 October 2021. An example of processing of personal data for monitoring purposes at the national level is the processing of personal data carried by the Italian Institute of Health (*Istituto Superiore di Sanità*) for the purposes of Epidemiological and microbiological surveillance in the context of the SARSCoV-2 epidemic (Covid-19). Further information is avalaible at: https://www.epicentro.iss.it/en/coronavirus/sars-cov-2-integrated-surveillance-data (accessed 22 October 2021).

[15] On this aspect see Ignacio Cofone, '*Immunity Passports and Contact Tracing Surveillance*' (2021) Stanford Technology Law Review 24, 176, 225 ss.; WIG Aponte (n. 5) 83.

[16] See art. 6 of the Reg. (EU) 2016/679 (GDPR).

[17] See art. 9 GDPR.

[18] A detailed analysis is provided in this paragraph; two example of such decisions are the following: Administrative Court of Zürich, AN.2020.00012, 3 December 2020; French Council of State, decision nn. 440442, 440445, 18 May 2020.

[19] See the decisions nn. 440442, 440445, of 18 May 2020 and no. 446155, 22 December 2020.

[20] French Council of State, decision nn. 440442, 440445, 18 May 2020.

[21] See point 4 of the decision.

[22] French Council of State, decision no. 440916 of 19 June 2020.

[23] The purposes were: i) the identification of persons infected with Covid-19 by ordering, performing and collecting the results of relevant medical examinations and providing evidence of clinical diagnosis; ii) the identification of persons who, having been in contact with them, are at risk of infection; iii) guidance of both to prophylactic medical isolation prescriptions and support during and after the end of these isolation measures; iv) national and local epidemiological surveillance as well as research on the virus and on ways to control its spread.

services can access the data.[24] However, the Council also concluded that social services are not allowed to process such data because their purposes are not directly connected to the pandemic, showing the need to establish both necessity and proportionality of the measures in relation to the pandemic. [25] Moreover, in another case, the French Council of State, assessing the lawfulness of data processing related to the use of thermal cameras in schools by municipal staff based on public interest reasons related to the pandemic, stated that there was a lack of a legal provision authorizing the processing.[26]

Some cases concerned the disclosure of data by public authorities to the general public or the duty of private parties to share personal data with public bodies. As to the former, the Constitutional Court of Montenegro decided a case concerning the constitutionality of a measure, taken by the national coordinating body for contagious diseases, to publish names and addresses of persons in self-isolation in relation to COVID-19 on the Government website to ensure the enforcement of rules on self-isolation.[27] This decision shows that Courts may separate the assessment on the legitimacy of the aim pursued through processing and the judgement concerning proportionality and necessity of the concrete measures adopted. [28] The Court, relying on European Court of Human Rights' case law, took into account the existence of a legitimate aim and its lawfulness, concluding that there was a legal basis for processing and that the aim of protecting public health is legitimate, considering the COVID-19 pandemic.[29] However, in assessing the necessity of the measure in a democratic society, the Constitutional Court of Montenegro found that such a measure did not strike a fair balance between the public health protection interests and the right to privacy .[30]

With regard to cases of data sharing from private parties to public authorities, in a decision on 15 February 2021, the Austrian DPA stated that the duty of private health centers to share negative results of PCR tests with public administration was justified because the processing was needed for developing the best strategy to combat the pandemic.[31] The DPA affirmed that the public interest reasons which justified the processing of health data may be specified by law or through an administrative act.[32]

As to cases where private parties process data, a decision of the Belgian Council of State concerns the obligation of restaurant clients to give the contact information of at least one person of their table. In this case, the Council considered the purposes of processing (*i.e.*, the building of an effective contact tracing system) as relevant for denying the existence of a danger to the fundamental right, which may have justified an urgency procedure.[33] In a similar case, the Austrian Constitutional Court stated that a municipal ordinance requiring restaurant owners to collect and share data for contact tracing purposes was not sufficiently justified with regard to the necessity and proportionality assessment, the latter being required by national law.[34]

Moreover, the processing of personal data within systems based on the so-called 'COVID certificates' is at stake in several decisions, where the legislative measures introducing such certificates are challenged.[35] As to Europe, in the EU, the Regulation 2021/953 of the European Parliament and of the Council, approved on 14 June 2021, establishes a framework for the issuance, verification, and acceptance of interoperable COVID-19 vaccination, test, and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic.[36] As to the case law, the French Council of State in an urgency procedure assessed the national legislation which allowed the French Prime Minister to require the presentation of the results of a negative test, of proof of vaccination status or recovery related to COVID-19, in order to allow some travels and the access to

[24] French Constitutional Council, decision 2020/800 of 21 May 2020.

[25] French Constitutional Council, decision 2020/800 of 21 May 2020.

[26] French Council of State, decision no. 441065, of 26 June 2020.

[27] Constitutional Court of Montenegro, decision no. U - II 22/20, of 23 July 2020.

[28] Constitutional Court of Montenegro, decision no. U - II 22/20, of 23 July 2020.

[29] Constitutional Court of Montenegro, decision no. U - II 22/20, of 23 July 2020.

[30] Constitutional Court of Montenegro, decision no. U - II 22/20, of 23 July 2020.

[31] Austrian DPA, Decision of 15 February 2021.

[32] Austrian DPA Decision of 15 February 2021.

[33] Decision no. 248.124 of 5 August 2020.

[34] See the decision of 10 March 2021, V 573/2020.

[35] On this issue, see: Alberto Alemanno and Luiza Bialasiewicz 'Certifying Health: The Unequal Legal Geographies of COVID-19 Certificates' (2021) European Journal of Risk Regulation 1.

[36] The text approved is available at: https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=celex%3A32021R0953 (accessed 26 June 2021). A comment to the regulation, published when it was still a proposal is provided for by Chiara Angiolini, 'Le proposte di Regolamento UE sul Certificato COVID digitale UE tra tutela della salute, libertà di circolazione e protezione dei dati personali', (2021) Biolaw Journal 2, 151.

certain places, establishments or events involving large gatherings of people for leisure activities or trade fairs.[37] In its decision, the Council of State affirmed the existence of a legal basis for processing under the GDPR[38], *i.e.*, the necessity of the processing for reasons of public interest in the area of public health. The Council of State took into account that i) the 'health pass' is likely to reduce the circulation of the Covid-19 virus in France by limiting the flow of people, ii) its use has been restricted to travel to foreign countries, Corsica and overseas, and to access to places of leisure, without affecting daily activities or the exercise of freedom of worship, assembly or demonstration.[39] The Spanish Supreme Court decided another case concerning national legislation regulating the use of COVID-19 certificates, within a procedure for the ratification of health measures restrictive of fundamental rights. The Court stated that limiting the access to certain inside entertainment establishments, where there is a large flow of people, to those persons who can prove that they are in possession of a valid 'COVID passport' must be ratified.[40] The Court considered that even if health data are processed, the pandemic situation, the massive vaccination, and the solidarity principle involved in protecting and helping each other prevails over privacy. As to the right to data protection, the Court stated that this right is not limited by the measure at stake, because the data are not collected as the data subject must only show the data for entry in the establishment.[41] Framing this decision in the light of the EU legislation, it should be recalled that under the GDPR the notion of "data processing" is broadly[42], and that also the access to the data for checking that the individual is in possession of the 'COVID passport' is a data processing under EU law.[43]

In Asia, the decisions vary. For instance, in India, the High Court of Orissa decided a case where the public disclosure of the identities of confirmed COVID-19 patients and persons in quarantine was implicated.[44] The Court concluded that the State Government approved measures to prevent unauthorized disclosure, and affirmed that the disclosure of the identity of such persons in exceptional circumstances of public health and safety concerns to the discretion of the State.[45] The Court in this case stated that disclosure is subject to scrutiny of a triple test developed in the case *K.S. Puttaswamy and another v. Union of India and others* (2017), where the Nine Judge Constitution Bench of the Apex Court stated that the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 of the Indian Constitution and as a part of the freedom guaranteed by Part-III of that Constitution.[46] The High Court of Orissa recalled that, according to *Puttaswamy*, the right to privacy is not absolute, as it can be subject to reasonable restrictions and the interference in such right can only be justified if "(i) the action is sanctioned by law; (ii) the action is aimed at achieving a legitimate aim; and (iii) the action is necessary and proportionate for the achievement of that aim". [47]

Furthermore, the exceptionality of the COVID-19 crisis was an element considered by the High Court of Kerala in its decision *Balu Gopalakrishnan & Anr. v. State of Kerala & Ors., W.P. (C). Temp No. 84,* 24 April 2020.[48] Here, the Government of Kerala affirmed that it could not continue the fight against COVID-19 without the assistance of software

[37] French Council of State, decision no. 453505, of 6 July 2021.

[38] Art. 9, para 2, lett. i) GDPR.

[39] French Council of State, decision no. 453505, of 6 July 2021, § 13.

[40] Spanish Supreme Court, no. 1112, 14 September 2021.

[41] Spanish Supreme Court, no. 1112, 14 September 2021.

[42] Art. 4, para 1, no. 2 GDPR defines processing as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".

[43] This interpretation is confirmed by EU legislation on the COVID certificate, which expressly regulates the cases where the data can be accessed for the purposes of the Regulation. In this respect, Art. 10 § 3 of the EU Regulation 2021/953 states that the personal data included in the certificates shall be processed by the competent authorities of the Member State of destination or transit, or by the cross-border passenger transport services operators required by national law to implement certain public health measures during the COVID-19 pandemic, only to verify and confirm the holder's vaccination, test result or recovery".

[44] High Court of Orissa, Cuttack, Ananga Kumar Otta v. Union of India & Ors., WP (C) No. 12430/2020, decision of 16 July 2020.

[45] High Court of Orissa, Cuttack, Ananga Kumar Otta v. Union of India & Ors., WP (C) No. 12430/2020, decision of 16 July 2020.

[46] High Court of Orissa, Cuttack, Ananga Kumar Otta v. Union of India & Ors., WP (C) No. 12430/2020, decision of 16 July 2020.

[47] High Court of Orissa, Cuttack, Ananga Kumar Otta v. Union of India & Ors., WP (C) No. 12430/2020, decision of 16 July 2020.

[48] High Court of Kerala, decision *Balu Gopalakrishnan & Anr. v. State of Kerala & Ors., W.P. (C). Temp No. 84,* 24 April 2020.

provided by a U.S. based company, and the the judges stated that they "do not think it will be prudent on our part, when our country and the whole world is fighting the pandemic, to issue any orders that would create a perception of impeding such effort". [49]

In South America, Brazil's Federal Supreme Court decided a case concerning the obligation, imposed by a provisional presidential decree, of telecommunication companies to share the list of names, telephone numbers, and addresses of their consumers with the Brazilian Institute of Geography and Statistics Foundation.[50] The Court stated that such a duty violates the right to intimacy and private life because the public entities had not proven the existence of a legitimate public interest to share personal data, considering the necessity, adequacy, and proportionality of the measure.[51] Moreover, the Federal Supreme Court took into account the fact that the guarantees of adequate and safe treatment of the shared data were absent.[52] In Colombia, the Constitutional Court undertook constitutional review of the Legislative Decree 458 of 2020, through which the National Administrative Department of Statistics was to provide, when requested, information collected in censuses, surveys, and administrative records to the State entities responsible for adopting measures to control and mitigate COVID-19. [53] The legislation provides that the data may only be used for these specific purposes.[54] The Court's reasoning relied on laws no. 1266/2008 and no. 1581/2012, which established the principles of purpose, freedom, and confidentiality in data processing and on the related case law.[55] Applying such principles to the case, the Court stated that data sharing between public bodies was legitimate because it aimed to ensure the minimum vital needs of the country's most vulnerable population, through their rapid identification.[56] Furthermore, the Court considered that data can be shared and further processed only to implement measures to control and mitigate the COVID-19, and even then only while the health emergency is in force.[57] In the facts of the case, data confidentiality was guaranteed and, accordingly, the Court stated that there was not a violation of the Constitution.[58]

In sum, where the legal grounds for processing consist in public interests related to the pandemic, the respect of data subjects' interests has been ensured through different means. First, in various cases concerning data processing by public authorities, Courts stated that the processing must be authorized by law[59] or at least by an administrative act.[60] Second, across continents, Courts applied the principles of necessity and proportionality balancing the fundamental rights and interests at stake.[61] Further research may compare the way Courts, across countries and continents, apply the principles of proportionality and necessity, separately or jointly. Such an analysis could be of particular interest for understanding whether and how the application of the principles differs across jurisdictions, and the consequences in terms of protection of fundamental rights of the various interpretations of such principles. Furthermore, from a comparative law perspective, this analysis could show the influences and relationships between legal systems and the existence of judicial dialogue between courts.

3.2. Data Subject's Consent

In an international landscape where the role of the data subject's consent in granting self-determination and fundamental rights is under discussion[62], a cluster of cases concern the role of

[49] High Court of Kerala, decision *Balu Gopalakrishnan & Anr. v. State of Kerala & Ors., W.P. (C). Temp No. 84,* 24 April 2020.

[50] Decisions ADI 6387 MC-REF of 24 April and 7 May 2020.

[51] Decisions ADI 6387 MC-REF of 24 April and 7 May 2020.

[52] Decisions of 24 April and 7 May 2020, ADI 6387 MC-REF.

[53] Constitutional Court, judgement C-150/20, 27 May 2020.

[54] Constitutional Court, judgement C-150/20, 27 May 2020.

[55] Par. 7.4 of the decision.

[56] Par. 8. 3.4 of the decision.

[57] Constitutional Court, judgement C-150/20, 27 May 2020.

[58] Constitutional Court, judgement C-150/20, 27 May 2020

[59] *E.g.*, French Council of State, 18 May 2020, nn. 440442, 440445; French Council of State, decision no. 441065, of 26 June 2020; Israeli decision 2109/20, *Ben Meir v. Prime Minister*, of 26 April 2020.

[60] E. g., Austrian DPA Decision of 15 February 2021.

[61] *E.g.*, French Council of State, 18 May 2020, nn. 440442, 440445; French Council of State, decision no. 440916 of 19 June 2020; French Constitutional Council, ; decision 2020/800 of 21 May 2020; Constitutional Court of Montenegro, decision no. U - II 22/20, of 23 July 2020; Austrian Constitutional Court, 10 March 2021, V 573/2020; High Court of Orissa, Cuttack, *Ananga Kumar Otta v. Union of India & Ors., WP (C)* No. 12430/2020, decision of 16 July 2020; Brazil Federal Supreme Court, Decisions ADI 6387 MC-REF of 24 April and 7 May 2020.

[62] See, for example: Laura Brandimarte, Alessandro Acquisti and George Loewenstein, *'Misplaced Confidences: Privacy and the Control Paradox'* (2012) Soc. Psyc. Per. Sc. 4, 340; Bart Willem Schermer, Bart Custers Simone van

consent with respect to the processing of health data during the pandemic. Obviously, Courts' trends in this field also vary depending on existing legislation. However, the case law shows that the data subject's consent is considered a legal tool for avoiding or limiting intrusive data processing.[63]

In Europe, data subjects' consent is a lawful ground for processing personal data, among others legal bases, such as, under certain conditions, the legitimate interest of the data controller or the public interest.[64] Moreover, consent must be freely given, specific, informed, and must consist of an unambiguous indication of the data subject's wishes, provided through a statement or by a clear affirmative action.[65] Furthermore, as health data is considered a special category of personal data, it is subject to specific rules for processing.[66] In particular, according to Art. 9 Reg. UE 2016/679, the processing of such data is prohibited, with some exceptions including the data subject's explicit consent.[67] In the case law, the French Council of State applied the health data regime in deciding the lawfulness of health data processing through a thermal camera in schools, recalling that one of the exceptions provided for by art. 9 of GDPR is data subject's explicit consent.[68]

Outside the EU, the Constitutional Court of Montenegro considered the role of data subjects' consent, assessing the constitutionality of the decision, taken by the National Coordinating Body for Contagious Diseases, to publish names and addresses of persons in COVID-19 self-isolation on the Government's website.[69] The Court relied on existing legislation, according to which health data may be processed only with the express consent of the person and when their processing is necessary for the purpose of detecting, preventing or diagnosing of data subject's illness or carrying out their medical treatment, as well as for the improvement of health services, in so far as the processing is done by a health worker or other person subject to the duties of keeping professional secret.[70] Relying on this legislation, the Court held that the health data was not processed according to the law, *i.e.* without the explicit consent of the person.[71]

As to Asia, in India, the High court of Karnataka stated that the use of a contact-tracing app (*Aarogya Setu*) must be voluntary and that personal data, and specifically health data, can be collected and further processed (*i.e.*, use and sharing) through this app only after the data subject has given her informed consent. The Court affirmed also that the benefits of any services that are provided by the Governments, its agencies, and instrumentalities must not be denied to an individual on the ground that she has not downloaded and installed the abovementioned app.[72] Furthermore, in a case concerning the use of a USA based software company for data processing by Government of Kerala, the High Court of Kerala, in a concise argument, stated that data may be accessed by the private company, or by other third-party service providers, only on the basis of citizens' specific consent.[73]

---

der Hof 'The crisis of consent: how stronger legal protection may lead to weaker consent in data protection' (2014) Eth. Inf. tech., 2; Marcin Betkier, *Privacy online, Law and the Effective regulation of online services* (Intersentia, 2019) 9.

[63] For some references to the critical debate on the effectiveness of consent for ensuring data subject's self-determination see footnote no. 66.

[64] See art. 6, Reg. (EU) 2016/679 (GDPR).

[65] See art. 6, art.7, art. 4 (11) Reg. (EU) 2016/679 (GDPR).

[66] See art. 9 Reg. (EU) 2016/679 (GDPR). In the European context, as to the special regime of health data, see the Council of Europe, *Recommendation CM/Rec(2019)2, Protection of Health-Related Data.*

[67] It should be recalled that to process lawfully special categories of data, both an exception to the prohibition in Art. 9 and a legal basis for processing among those provided for in Art. 6 EU Reg. 2016/679 must be applied. In other words, the processing of special categories of personal data falling under art. 9 GDPR should be made only if i) an exception to the prohibition of processing provided for by art. 9 GDPR is applicable and ii) a legal basis provided for by art. 6 GDPR applies. See in that regard: EDPB, 'Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art. 70.1.b))', of 23 January 2019, § 28, p. 8; EDPB, 'Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research', 2 February 2021, § 13; European Data Protection Supervisor, *'Preliminary Opinion 8/2020 on the European Health Data Space',* 17 November 2020, §§ 15-16).

[68] Decision no. 441065, of 26 June 2020.

[69] Constitutional Court of Montenegro, decision no. U - II 22/20, of 23 July 2020.

[70] On the Montenegro legal framework see: N Muftić, T Herenda, (n. 5).

[71] Constitutional Court, decision U - II 22/20, 23 July 2020. On that issue, although not mentioning the decision of the Constitutional Court, see N Muftić, T Herenda (n. 5).

[72] High court of Karnataka *Anivar A Aravind v. Ministry of Home Affairs, GM PIL WP (C) 7483 of 2020*, 25 January 2021

[73] *Balu Gopalakrishnan & Anr. v. State of Kerala & Ors., W.P. (C). Temp No. 84*, of 24 April 2020. On the relevance of consent in the Indian legal system, see: R Walters, L Trakman, B Zeller, *Data Protection Law. A Comparative*

3.3. The Intersections Between Public Interest and Consent as Legal Grounds for Processing

In two cases both the existence of a public interest ground and the data subjects' consent are addressed by Courts.

In Israel, the High Court of Justice decided the case 2109/20, *Ben Meir v. Prime Minister*, of 26 April 2020, where with regard to certain processing the ground is the public interest, while other processing operations are absed on consent.[74] The case concerned the legitimacy of a government decision providing the Israel Security Agency (ISA) authorization to process, for purposes of contact tracing, "technological information" regarding persons who tested positive to COVID-19, as well as persons who came into close contact with them .[75] With regard to processing based on public interests, the Court, taking into account the exceptional circumstances of the COVID-19 crisis, stated that if, in the future, the State seeks to continue to employ the means at the ISA's disposal, it must authorize such processing in primary legislation.[76] In this respect, in a subsequent judgment on the same issue, the Israeli High Court of Justice stated that the Government could not continue to authorize the ISA to assist in conducting epidemiological investigations in a sweeping manner. Furthermore, the Court affirmed that the Government must set criteria for situations in which ISA technology can be used.[77] Moreover, the Court stated that, from the time of its ruling, the government's ability to authorize to use of the ISA would be limited to cases where a person who tested positive for the virus does not cooperate in the human epidemiological investigation. [78]

However, in case no. 2109/20, *Ben Meir v. Prime Minister*, of 26 April 2020, the Court also provided specific rules concerning journalists, where consent plays a strong role. In particular, the High Court of Justice held, in the light of the fundamental importance of freedom of the press, that the contact tracing conducted by the State's preventive security service with especially intrusive means, particularly concerning journalists who tested positive for the virus, would require the consent of the data subject.[79] The Court stated that, in the absence of consent, a journalist would be required to undergo an individual epidemiological investigation, and would be asked to inform any sources with whom he was in contact over the 14 days before his diagnosis.[80]

In Europe, the High Court of Justice of Asturias decided a case concerning the obligation for hotels and restaurants to draw up and retain for 30 days an attendance list of attendees and for nightlife establishments a list of clients. The Court stated that the measure imposes a restriction of the right to data protection fir fighting the pandemic and that such measure is justified from an epidemiological point of view.[81] However, the Court stated that the measure is not proportional as it did not distinguish between situations where the risk of contagion is different. Accordingly, the Court affirmed that the administration must justify the necessity of the restrictions, being insufficient the generic statement on the need of ensuring social distance. The Court also mentioned some criteria (*e.g.*, the capacity of the premises, times of greater or lesser clients' flow, music installations that encourage shouting, the advantages and risks of terraces) the Administration should consider in justifying the restrictions.[82] In its proportionality test, the Court considered how the fundamental right to data protection is affected.[83] As a positive element for assessing the proportionality of the measure, the Court considered the consent of the data subject. In particular, the judges took into account that the measure did not impose a general obligation for data subjects to provide personal data, considering that data subjects must not provide personal data if they decide to not enter hotels, restaurants, or nightlife establishments.[84] The ruling is of particular interest in the light of EU law concerning consent as a legal basis for processing. In this regard, art. 7, § 4 of the GDPR states that in assessing whether consent is freely given, utmost account shall be taken of whether, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract. . Moreover, recital 42 of the GDPR states that "consent should not be

Analysis of Asia-Pacific and European Approaches, (Springer, 2019), 157.

74 High Court of Justice, decision 2109/20, *Ben Meir v. Prime Minister*, of 26 April 2020.

75 High Court of Justice, decision 2109/20, *Ben Meir v. Prime Minister*, of 26 April 2020.

76 High Court of Justice, decision 2109/20, *Ben Meir v. Prime Minister*, of 26 April 2020.

77 High Court of Justice, 6732/20 *Association for Civil Rights in Israel v. Knesset* 1 March 2021.

78 High Court of Justice, 6732/20 *Association for Civil Rights in Israel v. Knesset* 1 March 2021.

79 Decision 2109/20 *Ben Meir v. Prime Minister*, April 26, 2020.

80 Decision 2109/20 *Ben Meir v. Prime Minister*, April 26, 2020.

81 Asturias High Court of Justice, 10 June 2021, 15.

82 Asturias High Court of Justice, 10 June 2021, 19.

83 Asturias High Court of Justice, 10 June 2021, 15.

84 Asturias High Court of Justice, 10 June 2021, 15.

regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment".[85] In the light of these rules, if the data subject must provide personal data to enter in an establishment, her choice to enter in such establishment could not be qualified as a valid consent to the processing under EU law, because she is not able to refuse that consent without detriment. As an example, the detriment may consist in the prohibition of entry to restaurants. However, in assessing the proportionality of a measure, judges may consider whether the data subject may decide to not provide data as well as the consequences of such a decision (*e.g.*, deny of entry).

The qualitative analysis suggests that future research may concern the relationship between consent and other legal grounds for processing in different countries. For instance, future research could develop a comparison between cases where consent is considered the only legal ground for processing, and cases where other legal grounds exist (e.g. public interest). Such a study could also address the arguments used by the courts to justify a difference in the regime for processing personal data (e.g., the need to obtain consent to the processing, not using public interests grounds depends on a greater risk of violation of fundamental rights at stake through processing, or to scientific uncertaintly relating to the need of the processing for protecting public and collective health).

4. The Aspects of Data Processing Taken into Account in Courts' Reasoning

When deciding on the lawfulness of data processing or on the measures authorizing it, Courts consider not only the grounds or the purpose for processing, but also the concrete characteristics of the processing operations. This paragraph illustrates the different aspects that the Courts took into account in their reasoning. Adopting a bottom-up approach, the following aspects may be identified: i) data categories; ii) data retention period; iii) subjects who can access data; iv) means of processing; and v) consequences of processing with respect to the data subject.

4.1. Data Categories

Health data plays a major role in processing personal data for facing the pandemic. As to the definition of this category of data in the context of the current health crisis, in Europe the Austrian DPA, in the light of the EU Court of Justice's caselaw (*Lindqvist*, C-101/01), affirmed that the notion of health data should be interpreted broadly.[86] In Poland, the DPA stated that the notion of health data encompasses information about the quarantine of a person who was exposed to a disease or who has been in contact with a source of a biological pathogen.[87] The Polish DPA also concluded that whether or not the person exhibits disease symptoms is irrelevant for this qualification.[88] In the same vein, the Constitutional Court of Montenegro, applying national law, found that personal data of persons in self-isolation, where their health condition was monitored by the competent authority, have to be qualified as health data because they concern the risk of becoming ill or of having been exposed to COVID-19 virus[89]. In the same decision, the Constitutional Court of Montenegro stated that medical data requires special protection. [90] A similar argument was used by the French Constitutional Council in the abovementioned decision no. 2020/800 of 21 May 2020, where the Council stated that when personal data of a medical nature is processed, particular attention must be paid in the processing and in the definition of its boundaries.[91]

Furthermore, in a decision concerning a measure concerning the obligation for hotels, restaurants, and other establishments to collect personal data of attendees or clients, the High Court of Justice of Asturias took into account the nature of data collected in assessing the proportionality of the measure. In particular, the Court relying on a decision of the Spanish Constitutional Tribunal[92], stated that the categories of data collected are "peripheral and innocuous data" in relation to the data subjects' privacy, at least in the light of the interests at stake, in this case, the health and life of data subjects.[93] In this vein, the Administrative Court of Zürich adopted similar reasoning in an analogous case: the Court stated that there was only

[85] On the interpretation of these rules the debate is open. See Court of Justice of the EU, *Orange Romania*, C-61/19, 11 November 2020; EDPB Guidelines 5/2020 on consent under regulation 2016/679, 4 May 2020; Lee A. Bygrave, 'Art. 4(11) Consent' in Christopher Kuner and others (eds.), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press, 2020); E. Kosta 'Art. 7 Conditions for consent', *ibidem*.

[86] Austrian DPA, decision of 15 February 2021.

[87] Decision of 12 November 2020, no. DKN.5101.25. 2020.

[88] Decision of 12 November 2020, no. DKN.5101. 25.2020.

[89] Decision no. U - II 22/20, of 23 July 2020.

[90] Decision no. U - II 22/20, of 23 July 2020.

[91] French Constitutional Council, decision no. 2020/800 of 21 May 2020.

[92] Spanish Constitutional Tribunal, no. 97, 17 July 2019.

[93] Asturias High Court of Justice, 10 June 2021.

minimal interference with the right to informational self-determination because of the nature of the data processed (surname, first name, postcode, mobile phone number, e-mail address, time of entry and exit to the catering establishment).[94]

Moreover, the relation of strict necessity between the purposes and the definition of data category to be processed is evaluated as a positive element within the assessment of the constitutionality of measures challenged. For example, the French Council of State, in a case concerning the processing of personal data within the COVID-19 Certificates System, affirmed that the processing of identification data is necessary to check that the pass presented is that of the person presenting it.[95] Furthemore, this issue emerged in contact tracing cases across continents. For example, in Europe, in its decision of 15 June 2020 the Norwegian DPA relied on the *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*, adopted on 21 April 2020 by the European Data Protection Board, stating that the use of location data in contact tracing is unnecessary and recommending the use of Bluetooth data only. Accordingly, the Norwegian DPA stated that the Norwegian authority had not sufficiently justified the need to use location data for contact tracing. In India, the High Court of Orissa, assessed the necessity of public disclosure of patient's names by public authorities, considering whether the processing of information concerning a COVID-19 patient's identity led to better and more comprehensive contact tracing, taking into account the right to privacy and the social stigma and discrimination suffered by persons infected or suspected of being infected by COVID-19.[96] A similar argument, concerning the risk of stigmatization derived from the publication of a list of persons in quarantine was adopted by the Constitutional Court of Montenegro.[97] Lastly, Courts considered the categories of data processed assessing the risks concerning data transfers outside external borders, showing the relevance that the kind of data processed may adquire in Courts' reasoning concerning the protection of fundamental rights and data subject's interests.[98]

In sum, in relation to the categories of data, three legal issues arise: the notion of health data, the relationship of necessity between the purposes of processing and the definition of the data processed, and the relevance of the nature of data in assessing the impact of the processing on the right to privacy and data protection.

With regard to the first aspect, within the case law concerning the processing of data for facing the pandemic, the issue of the boundaries of the notion of health data is at stake, and Courts – at least European courts – seem to adopt a broad interpretation of this concept. From the perspective of future research, a comparison between the notion of health data adopted by the courts before and during the pandemic may be developed for understanding if the notion is evolving within the case law.

Secondly, the relationship of necessity between the purposes of processing and the definition of the data processed is an important aspect of decisions of European and Indian Courts. In this respect, further research may consider how the necessity test is conducted across countries. In that regard, the Indian case shows that the necessity assessment could encompass not only the need for processing in relation to the purposes but also the risks for data subjects' fundamental rights involved in such processing.

Lastly, in relation to the relevance of the nature of data in the Courts' assessment concerning the impact of the processing on the right to privacy and data protection, further research may concern the criteria with which the consequences of the processing of different categories of data are compared and assessed.

4.2. Data Retention Period

The data retention period is another element considered by Courts, across all continents analyzed, in the assessment of the balancing choices made within data processing or with respect to provisions regulating such processing. This period is often mentioned by Court, but the way it is relevant is often not explicit in judges' reasoning.[99] In cases concerning data processing for contact tracing purposes, in India the High Court of Kerala

[94] Administrative Court of Zürich, AN.2020.00012, 3 December 2020, § 4.5.2.

[95] French Council of State, decision no. 453505, of 6 July 2021, § 8.

[96] High Court of Orissa, *Ananga Kumar Otta v. Union of India & Ors, WP (C)*, No. 12430/2020, of 16 July 2020.

[97] Decision no. U - II 22/20, of 23 July 2020.

[98] French Council of State, decision of 12 March 2021, no. 450163. In that case the data processed included personal identification data and data relating to appointments, but no health data on the possible medical grounds for eligibility for vaccination.

[99] *E.g.*, High Court of Kerala, decision of *Ramesh Chennithala vs State of Kerala* of 21 August 2020.

found that data are destroyed after 14 days.[100] In Europe, the Belgian Council of State, in its decision 248.124 of 5 August 2020, considered the data retention period (14 days) as an element for evaluating the conditions of gravity necessary for deciding the case in an urgency procedure.[101] In Switzerland, the same retention period was considered by the Administrative Court in assessing the proportionality of a measure that established the obligation for accommodation and catering services to collect data of their guests for contact tracing purposes.[102] In France, the Council of State considered the retention period in order to evaluate the risks related to data transfers.[103] In Spain, the High Court of Justice of Asturias considered the retention period in assessing the proportionality of a measure concerning the obligation for hotels, restaurants, and other establishments to collect personal data of attendees or clients.[104]
In one case, the necessity of the data retention period in relation to the purposes of processing is considered: in Brazil, the Supreme Court held that the conservation of personal data collected by the public entity was manifestly in excess of the strictly necessity to fulfill its stated purpose.[105]

In sum, Courts considered the data retention period as a relevant element but often they do not specify the arguments of such relevance; this is a critical aspect of the analysed decisions, as the reasons for the assessment of the data retention period could be explained in the decisions (e.g. a long retention period raises the risk of infringement of the data subject's rights; the retention period is necessary – or not – for the purposes of the processing).

4.3. Subjects Who Can Access Data

Courts took into account the number and the kind of subjects who can access data and the relationship between who processes data and the data subject. As to the level of disclosure and confidentiality of data, the Constitutional Court of Montenegro took into account the fact that personal medical data were made publicly accessible to an indefinite number of persons on the internet when assessing the respect of the necessity in a democratic society of the Government's decision of publishing names and addresses of persons in self-isolation in relation to COVID-19.[106] In Spain, the provision of only one public body – the Directorate General for Public Health – who can process personal data for contact tracing purposes is an element considered by the High Court of Justice of Asturia in assessing the proportionality of a measure concerning the obligation for hotels, restaurants, and other establishments to collect personal data of attendees or clients.[107] In India, the confidentiality of personal data related to COVID-19 (*i.e.*, the absence of public disclosure and the limitation of subjects who can access data) is a key element in the decision *Balu Gopalakrishnan & Anr. V. State of Kerala & Ors*., W.P. (C) of the High Court of Kerala. In this case, the Court ordered a company providing software that processes and analyse patients data and data concerning persons vulnerable to the COVID to the Government not to commit any act which would be, directly or indirectly, in breach of confidentiality of the data entrusted to it for processing by the Government of Kerala and to not disclose such data to any third party.[108] Moreover, confidentiality is a relevant aspect in the reasoning of another decision from the same court, *Ramesh Chennithala vs State of Kerala*, of 21 August 2020. The case concerned the collection of Call Detail Records (CDR) by the police to track where patients were 14 days before they were confirmed to be positive and the Court dismissed the action, taking into account the strict confidentiality of CDR.[109] Furthermore, the public disclosure of the identity of confirmed COVID-19 patients was at stake in the case decided by the High Court of Orissa, where, although the Court rejected the claim, it acknowledged that the level of disclosure of personal data had an impact on the protection of the right to privacy. [110]

Regarding the kind of subjects who can access data, in Israel the High Court of Justice concluded that the violation of privacy was particularly severe because of the institution that processes data, the Israel Security Agency (ISA), which was in charge of tracking the State's citizens and residents. The Court found that this entity normally act for fighting

[100] High Court of Kerala, decision of *Ramesh Chennithala vs State of Kerala* of 21 August 2020.

[101] Belgian Council of State, decision 248.124 of 5 August 2020.

[102] Administrative Court of Zürich, AN.2020. 00012, 3 December 2020, § 4.5.2.

[103] Decision of 12 March 2021, no. 450163. The maximum retention period provided for data concerning the vaccination appointment was three months.

[104] Asturias High Court of Justice, 10 June 2021, 17.

[105] Decisions ADI 6387 MC-REF of 24 April and 7 May 2020.

[106] Decision U - II 22/20, of 23 July 2020.

[107] Asturias High Court of Justice, 10 June 2021, 17.

[108] High Court of Kerala, *Balu Gopalakrishnan & Anr. v. State of Kerala & Ors*., W.P. (C), Temp No. 84, 24 April 2020.

[109] High Court of Kerala, *Ramesh Chennithala vs State of Kerala*, of 21 August 2020.

[110] High Court of Orissa, *Ananga Kumar Otta v. Union of India & Ors., WP (C)*, No. 12430/2020, 16 July 2020.

against hostile elements, while in the present case its means were used in relation to "citizens and residents who do intend it no harm".[111] The Court took into account also that data processing by this kind of subject is exceptional in the international landscape.[112]

In India the specific relation between doctor and patient and the regulation of the information received by the doctor during this relationship was considered as a relevant element by the High Court of Orissa, which assessed the compatibility of the disclosure of the identity of the confirmed COVID-19 patients with the right to privacy.[113] In particular, the Court relied on national and international legislation and on previous case law in affirming that confidentiality in the relationship between a doctor and her patients is a key rule, with few exceptions which should be provided by law. One of these exceptions is based on the public interest of the information.[114]

4.4. The Means of Processing

The means of processing operations are of particular importance in some Courts' reasonings. In France, the Council of State, in its decision concerning the processing of personal data within the Covid-19 certificates system, analysed in detail how the processing is carried out (the use of a QR code and of a decentralised system) for affirming the respect of the principle of data minimization.[115]

In the Israeli case decided by the High Court of Justice, 2109/20 *Ben Meir v. Prime Minister*, of 26 April 2020, the Court found that the violation of privacy is particularly severe because of the chosen means of processing.[116] Such means are under secrecy by reason of the "desire to preserve secrecy in regard to the ISA's abilities". The Court stated that the use of the same tools used by the security agency against hostile elements with respect to the State's citizens and residents who do not intend to harm is a threat to democracy.[117] Moreover, the Court took into account: i) the importance of transparency of the means of processing, lacking in the present case; ii) the lack of consent; and iii) the need to make an effort to find "alternatives like those adopted elsewhere in the world, among them, use an application developed by the Ministry of Health, which are all based upon obtaining the consent of the person being tracked".[118] As to the existence of other ways to obtain the same objectives, a similar argument was used by the French Council of State, in its decision no. 440916 of 19 June 2020.[119] In this decision, the Council stated that the processing of health data within a national data hub to conduct projects of public interest in relation to the pandemic can be justified, *inter alia*, where alternative solutions are lacking.[120]

Furthermore, the tracking means evaluation used by the State's preventive security service at the core of the Israeli decision no. *6732/20 Association for Civil Rights in Israel v. Knesset,* decided by the High Court of Justice on 1 March 2021.[121] In this decision, the majority

[111] Decision 2109/20 *Ben Meir v. Prime Minister*, of April 26, 2020. The Court stated that "The violation of privacy in the present case is particularly severe for two primary reasons: The first concerns the identity of the entity that is exercising the means under discussion, that is, the fact that it is the ISA – the State's preventive security service – that is tracking the State's citizens and residents, and the second concerns the nature of the means chosen, viz., the fact that we are speaking of a coercive mechanism that is not entirely transparent. "As for the identity of the entity employing the said means – employing tools that were developed for the purpose of fighting against hostile elements, and aiming them at the State's citizens and residents who do intend it no harm is a step that might cause any lover of democracy to lose sleep", par. 38.

[112] Decision 2109/20 *Ben Meir v. Prime Minister*, of April 26, 2020. The Court stated that "To this we may add that according to documents published by the Israel Democracy Institute (hereinafter: the Institute), the apparatus employed in Israel that will be used to locate contacts with validated patients is carried out with the aid of the preventive security organ, is exceptional on the international landscape", par. 38.

[113] Decision *Ananga Kumar Otta v. Union of India & Ors., WP (C)*, No. 12430/2020, 16 July 2020.

[114] Decision *Ananga Kumar Otta v. Union of India & Ors., WP (C)*, No. 12430/2020, 16 July 2020, par. 11-12.

[115] French Council of State, decision no. 453505, of 6 July 2021, § 9.

[116] High Court of Justice, 2109/20 *Ben Meir v. Prime Minister*, of 26 April 2020.

[117] High Court of Justice, 2109/20 *Ben Meir v. Prime Minister*, of 26 April 2020.

[118] Para. 40 of the decision of the Israeli High Court of Justice, 2109/20 *Ben Meir v. Prime Minister*, of 26 April 2020.

[119] French Council of State, decision no. 440916 of 19 June 2020.

[120] French Council of State, decision no. 440916 of 19 June 2020.

[121] On both decisions see: E Albin, I Bar-Siman-Tov, A Gross, T Hostovsky brandes, 'Israel: Legal Response to COVID-19, in The Oxford Compendium of National Legal Responses to Covid-19', (updated April 2021) (available at: https://oxcon.ouplaw.com/view/10.1093/law-occ19/law-occ19-e13#law-occ19-e13-note-270; (accessed 11 June 2021); on the decision of 1st March 2021, see Tamar Hostovsky Brandes 'Tracking Citizens. Military Surveillance Tools in Israel and Privacy in a Pandemic' (22 March 2021) Verfassungsblog <https://verfassungsblog.de/tracking-citizens/> accessed 11 June 2021.

opinion held that it is disproportionate and unreasonable to use the ISA tool that collects sensitive information in a sweeping manner.[122] The Court took into account the fact that the government had not established measurable criteria for implementing the measure, even if the concrete situation evolved (*e.g.*, the vaccination campain, the claim of the ISA that the use of the tool should be reduced).[123] The Court stated the tracking tool should be interpreted by the Governement as its last resort, and, where necessary, it could be used as a complementary tool only for individual cases.[124] Accordingly, the Court stated that the surveillance can be carried out only after the governmental definition of measurable criteria for determining the scope of the complementary use of the ISA tool, and that such surveillance must be limited only to those who won't cooperate with epidemiological investigations. [125]

4.5. Consequences of Processing with Respect to the Data Subject

In some cases Courts considered the consequences of processing with respect to the data subject. For instance, the Constitutional Court of Montenegro, in its decision U - II 22/20, of 23 July 2020, evaluated the necessity in a democratic society of the Government's decision consisting of the publication of names and addresses of persons in self-isolation due to COVID-19 on the Government's website[126]. The Court considered the consequences of processing with respect to the data subject, namely that a consequence of data disclosure could be that those in need of medical assistance might have been deterred from seeking appropriate treatment, thereby endangering their own health and eventually public health.[127]

Moreover, the French Council of State, in its decision concerning the processing of personal data within the Covid-19 certificates system, assessed the risk to the rights and freedoms of natural persons that the processing may create in the light of the EU legislation concerning the data protection impact assessment.[128] In this regard, art. 36 GDPR provides that the data controller shall consult the supervisory authority prior to processing where the data protection impact assessment indicates that the processing would result in a high risk, in the absence of measures taken by the controller to mitigate the risk. The French Council of State affirmed that the violation of the prior consultation of the national DPA is likely to constitute a serious and manifestly unlawful breach of the right to privacy and personal data protection.[129] However, the Council stated that in the present case there was not a violation of such prior consultation rule, taking into account that the risks related to illegitimate access to and unwanted modification of data were mitigated by the following elements: i) the processing was based on local control of the data ("off-line mode"); ii) the government did not exchange data with the central server of the service provider company when verifying the receipts presented on the mobile phone of the person intending to use the COVID certificate.[130]

In Poland, the DPA found that the ways in which the controller's failure to comply with legal obligations concerning data security may have an impact on data subjects' rights and freedoms.[131] In particular, the DPA stated that the nature, scope, context, and purposes of the processing and the risk of violation of the rights or freedoms are factors that the data controller must take into account in building the data protection system[132]. In this case, the DPA found that within the processing risk analysis, the data controller must take into account the existence of the COVID-19 pandemic, the sense of fear associated with the epidemiological situation, and the potential harms stemming from the unlawful disclosure of personal data related to COVID-19, such as discrimination, stigmatization, social ostracism, stress, and potential material

[122] Israeli High Court of Justice, no. *6732/20 Association for Civil Rights in Israel v. Knesset,* 1 March 2021.

[123] The analysis of this case is based on a case summary drafted by prof. Dr. Ittai Bar-Siman-Tov & Yehonatan Dayan & Shaiel Tchercansky in the framework of the Covid-19 Litigation project.

[124] Israeli High Court of Justice, no. *6732/20 Association for Civil Rights in Israel v. Knesset,* 1 March 2021.

[125] Israeli High Court of Justice, no. *6732/20 Association for Civil Rights in Israel v. Knesset,* 1 March 2021.

[126] Constitutional Court of Montenegro, decision U - II 22/20, of 23 July 2020.

[127] Constitutional Court of Montenegro, decision U - II 22/20, of 23 July 2020.

[128] French Council of State, decision no. 453505, of 6 July 2021, § 10.

[129] French Council of State, decision no. 453505, of 6 July 2021, § 10.

[130] French Council of State, decision no. 453505, of 6 July 2021, § 10.

[131] Decision of 12 November 2020, no. DKN.5101.25.2020.

[132] Decision of 12 November 2020, no. DKN.5101.25.2020.

losses derived from the negative reaction of the community where the data subject lives[133].

4.6. Summing up: the Relevance of Concrete Characteristics of the Processing Operations in Courts' Reasoning

A transversal issue to the different aspects considered by the Courts is that of the organization of interests around personal data: mainly those of data subjects and those of the public linked to the fight against the pandemic. The need to coordinate several interests emerges in the analysis of different aspects of concrete data processing operations. In certain cases, the Courts' reasoning is specific to one aspect of data processing: i) in relation to the category of data Courts and DPAs affirmed that medical data need specific protection[134]; ii) the gravity of the violation of privacy was assessed relying on the kind of subject who process data[135]; and iii) the Court examined the possibility to put in place alternative and less intrusive means of processing[136]. However, coordination between different interests sometimes occurs through the principles of necessity and proportionality. Necessity is applied in assessing the relationship between the purposes of processing and i) the definition of the category of data to be processed[137]; ii) the data retention period[138]; iii) the level of disclosure and of confidentiality of data[139]; and iv) the consequences of processing with respect to the data subject[140].

In some cases, Courts applied the principle of proportionality, for example with regard to the means of processing[141]. Moreover, in at least one case, necessity, proportionality, and the data minimization principle are considered jointly in the assessment concerning the category of data processed[142]. The analysis shows that further research may be conducted in order to analyse how, across countries, the various aspects of processing are part of the necessity or proportionality tests, and which are the consequences of the possible differences in the outcomes of the decisions, particularly in relation to the level of data subjects' protection.

5. Data Transfers to Third Countries

Another issue that emerged in the case law concerning the processing of personal data relates to the data transfers outside external borders. Generally speaking, this topic is a crucial one in data protection law; however, the analysis of the few cases where such data transfers were part of data processing operations aimed at combatting the pandemic is a starting point for building a comparison of case law prior to and contemporaneous with the pandemic.

In India, in the decision *Balu Gopalakrishnan & Anr. v. State of Kerala & Ors., W.P. (C).* Temp No. 84, of 24 April 2020, the High Court of Kerala took into account the possibility of data transfers, stating that a USA-based software company who concluded with the Kerala Government a contract concerning data processing "shall not disclose (…) such data to any third party/person/entity – of whatever nature or composition – anywhere in the world".

In Europe, although not related to the processing of data for purposes related to COVID-19, the judgment *Schrems Facebook Ireland*, C- 311/20, of 16 July 2020 issued by the Court of Justice of the European Union (CJEU), is relevant to frame national decisions related to data transfers in the context of the pandemic.[143] For the purposes of this article, it should be recalled that in *Schrems Facebook Ireland,* (C-311/20) the CJEU, relying on its previous case law (*Schrems*, C-362/14), on the principle of proportionality, and on art. 52 of the Charter of Fundamental Rights of the EU concerning the limits of fundamental rights, stated that the Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 on the adequacy of the protection provided by the *EU-US Privacy Shield*, was invalid.[144] Furthermore, in its judgement, the Court concluded that data subjects whose personal data are transferred to a

[133] Decision of 12 November 2020, no. DKN.5101.25.2020.

[134] See: Constitutional Court of Montenegro, in its decision no. U - II 22/20, of 23 July 2020; Austrian data protection authority, decision of 15 February 2021.

[135] Israeli High Court, 2109/20 *Ben Meir v. Prime Minister*, of April 26, 2020.

[136] Israeli High Court of Justice, 2109/20 *Ben Meir v. Prime Minister*, of April 26 2020; French Council of State, in its decision no. 440916 of 19 June 2020.

[137] For example, see French Constitutional Council, decision no. 2020/800 of 21 May 2020; High Court of Kerala, *Ramesh Chennithala vs State of Kerala*, of 21 August 2020; Norwegian DPA, decision of 15 June 2020.

[138] See: Brazilian Supreme Court, decisions ADI 6387 MC-REF of 24 April and 7 May 2020.

[139] For example, see Constitutional Court of Montenegro, decision no. U - II 22/20, of 23 July 2020; High Court of Kerala, *Balu Gopalakrishnan & Anr. v. State of Kerala & Ors*., W.P. (C). Temp No. 84, 24 April 2020; French Constitutional Council, dec. no. 2020/800 of 21 May 2020.

[140] Constitutional Court of Montenegro, decision U - II 22/20, of 23 July 2020.

[141] Israeli High Court of Justice, *6732/20 Association for Civil Rights in Israel v. Knesset,* 1 March 2021.

[142] French Council of State, no. 440916, 19 June 2020.

[143] CJEU, judgment *Schrems Facebook Ireland*, C-311/20, of 16 July 2020.

[144] CJEU, judgment *Schrems Facebook Ireland*, C-311/20, of 16 July 2020. That EU Commission Decision allowed, under certain conditions, the free transfer of data to companies certified in the US.

third country must be afforded a level of protection essentially equivalent to that guaranteed within the European Union by the GDPR, read in the light of fundamental rights. [145] To that end, the Court stated that the assessment of the level of protection afforded in the context of such a transfer must consider: i) the contractual clauses between the controller or processor established in the European Union and the recipient of the transfer established in the third country concerned; and ii) the relevant aspects of the legal system of that third country with regard to any access by the public authorities of that third country to the personal data transferred. [146]

The *Facebook Schrems* case (C-311/18) had an impact in national litigation related to COVID-19, as shown by the the French case law concerning the hosting subcontracting for the "Health data hub" made by French authorities. In a first decision, no. 440916, of 19 June 2020, prior to *Facebook Schrems* case (C-311/18), the Council of State, *inter alia*, stated that data transfers to the USA for maintenance needs complied with the GDPR, as they were authorized by a decision of the European commission in 2016, which the GDPR allows[147]. In its second decision on the same topic the Council of State, given the possibility of data being transferred to the United States, deeply analyzed (i) the risk of data transfers due to the application of the contract with Microsoft; and (ii) the risk of other types of data transfers (extraterritoriality of US law).[148]

An interesting case was decided by the French Council of State in decision no. n°450163, of 12 March 2021, where associations and trade unions asked the interim relief judge of the Council of State to suspend the partnership between the Ministry of Health and Doctolib, arguing that the hosting of vaccination appointment data by the subsidiary of a US company (Amazon Web Services) entailed risks with regard to access requests by the US authorities.[149] The Council of State, applying the criteria laid out by the CJUE in its judgment *Schrems Facebook Ireland* (C-311/18) of 16 July 2020 to the relationship between controller and processor, decided that the level of protection provided during the data processing should be verified by taking into account not only the contractual stipulations between the controller and the processor, but also, in the event of the processor being subject to the law of a third country, the relevant elements of the legal system of that country.[150] Taking into account existing safeguards and the data categories concerned, the Council of State found that the level of protection of data relating to appointments made in the context of the COVID-19 vaccination
campaign is not manifestly inadequate in the light of the risk of infringement of the GDPR invoked by the applicants.[151] Therefore, the Council of State held that the decision of the Minister of Solidarity and Health to entrust the company Doctolib, among other possible ways of booking appointments, with the management of covid-19 vaccination appointments does not seriously and manifestly illegally infringes the right to respect for private life and the right to protection of personal data.[152]

In the analyzed case law the Court's approaches vary. In an Indian case, the Court affirmed that the obligation of confidentiality applies globally to every subject, while the European approach focuses on the level of protection in the third country. However, the analysed case law does not attach particular importance to the pandemic context for deciding the questions related to the pandemic. Future litigation on this topic may concern possible cases where data transfers may pursue the public interest concerning the fight of the pandemic (e.g., scientific research or the coordination of vaccination campaign based on health data), and there are significant risks for data subjects' rights (*e.g.*, the risk of surveillance by the foreign country).[153]

6. Remedies

An important aspect of case law analysis is the one concerning the remedies provided by Courts. In the following table, the remedies granted by the courts are described and grouped in categories. Such categories have been defined through a bottom-up approach: from the reading of the decisions and their comparison a grouping of the case law has been made, for providing a first overview of the remedies adopted, including through the drafting of the following table.

[145] CJEU, judgment *Schrems Facebook Ireland*, C-311/20, of 16 July 2020.

[146] CJEU, judgment *Schrems Facebook Ireland*, C-311/20, of 16 July 2020.

[147] Council of State, decision no. 440916, of 19 June 2020.

[148] French Council of State, n°444937, of 13 October 2020.

[149] French Council of State, decision no. n°450163, of 12 March 2021.

[150] French Council of State, Council of State in decision no. n°450163, of 12 March 2021.

[151] French Council of State, decision no. n°450163, of 12 March 2021.

[152] French Council of State, decision no. n°450163, of 12 March 2021.

[153] On this issue, see Heidi Beate Bentzen and others 'Remove obstacles to sharing health data with researchers outside of the European Union' (2021) Nat. Med. 27, 1329.

DECISION	REMEDY APPLIED	CATEGORY OF REMEDY
Austria, Constitutional Court, V 573/2020 10 March 2021,	The Court stated that there was a lack of formal requirements with respect to the challenged measures.	Declaration of unconstitutionality
France, French Constitutional Council decision no. 2020/800 21 May 2020	Partial declaration of unconstitutionality. The Court declared the following provisions against the Constitution: - the sharing of data with social service, for the lack of a direct link with the fight against the pandemic; - the subordination of the regulatory power of the prime minister to the one of another authority (national DPA).	
Montenegro, Constitutional Court of Montenegro, decision U - II 22/20, 23 July 2020	The Decision, adopted by National coordinating body for contagious diseases, to publish names and addresses of persons in self-isolation due to COVID-19 on the Government's website, without their consent, violated their right to respect their private life.	
Brazil, Federal Supreme Court ADI 6387 MC-REF, 7 May 2020	The Court declared the unconstitutionality of the provision enabling data sharing from telecommunication companies to the Brazilian Institute of Geography and Statistics, due to the violation of the right to intimacy and private life.	
Spain, Supreme Court, no. 1103, 18 August 2021	The Court rejected the claim against the reject of ratification of a measure that limited the access to inside entertainment and hospitality establishments with music to those persons who can prove that they have a valid EU Covid digital certificate or accreditation of antigen test or negative PCR. The Court stated that the measure is not proportional as it is neither necessary nor adequate. The Court took into account the limitation of the right to personal privacy provided for by the measure in its proportionality assessment.	Rejection of the ratification imposing limitations to fundamental rights. (or rejection of the claim against the rejection of ratification)
Spain, Asturias High Court of Justice, 10 June 2021	The Court rejected ratification of measures which imposed the obligation to draw up and retain for 30 days an attendance list for hotels and restaurants and a list of clients for nightlife establishments. The Court considered that the measure was not proportional as it not distinguished between situations where the risk of contagion is different. Accordingly, the Court considered that the Administration must specify the necessity of the restrictions.	
Brazil, Federal Supreme Court ADI 6387 MC-REF, 24 April 2020	The Court, in an urgency procedure, on the basis of the necessity to prevent irreparable damage to the intimacy and privacy of more than a hundred million users of fixed and mobile telephone services, suspended the provision enabling processing, determining that the Brazilian Institute of Geography and Statistics must refrain from requesting to the telephone companies the access to list of names, telephone numbers and addresses of the consumers.	Suspension in an urgency procedure of the effectiveness of the measure enabling processing, with the effect of prohibiting such processing
India, The High Court of Orissa, Cuttack, Ananga Kumar Otta v. Union Of India & Ors, WP (C) No. 12430/2020, 28 May 2020	The court stated that the State authorities must ensure that the identity of any person, who is admitted to COVID centers, any Government Hospital/private Hospital or any Quarantine center in the State, found infected with Coronavirus (COVID-19) is not disclosed/publicized either in any intra-departmental communication or in any media platform including social media.	Temporary prohibition of processing
Norway, Data Protection Authority, decisions of 15 June and 17 August 2020	Temporary ban on the processing of personal data within a contact tracing app.	
France, Council of State, dec. decision nn. 440442, 440445; 18 May 20220; Council of State, decision no. 446155, 22 December 2020,	The Council of State, in its decision of 18 May 20220, nn. 440442, 440445, ordered the State to immediately cease drone surveillance concerning compliance with the health regulations in force during the COVID-19 emergency. This decision was confirmed in the decision of 22 December 2020, n°446155.	Prohibition of processing

France, Council of State, decision no. 441065, 26 June 2020	The Council of State ordered the municipality of Lisses to cease the use of portable thermal imaging cameras deployed in schools.	
Poland, Data protection authority, decision no. DKN.5101.25.2020, 12 November 2020,	The DPA stated that, as there was a breach of data confidentiality which implies a high risk of a violation of rights or freedoms of natural persons, the data controller is obliged to notify the data subjects of the breach of protection of their personal data without undue delay.	Ascertainment of the existence of a data breach and related obligations
India, High Court of Kerala, *Balu Gopalakrishnan & Anr. v. State of Kerala & Ors.,* W.P. (C). Temp No. 84, 24 April 2020	The Court issued some order related to the measures for ensuring the confidentiality of data. The Court: - ordered to the Government of Kerala: i) to anonymize all the citizens' data related to the COVID-19 pandemic collected or to be collected; ii) to allow the USA-based software company to have further access only to such anonymized data; iii) to inform every citizen concerned that such data is likely to be accessed by third party service providers and iv) to ask for their specific consent for the latter processing. - The Court ordered the USA-based company: i) to not commit any act which would breach the confidentiality of data shared with them for processing by the Government of Kerala under the challenged contract; ii) to not communicate such data to any third party anywhere in the world; iii) to give back all such data to the Government of Kerala as soon as the contractual obligation, as regards its processing, is performed; iv) to give back to the Kerala Government any residual or secondary data available; and v) to not use or exploit any such data, or the name and the official logo of the Government of Kerala, directly or indirectly, for any commercial benefit.	The Court partially upheld the claim and gave some prescriptions on data processing operations
India, High court of Karnataka, *Anivar A Aravind v. Ministry of Home Affairs, GM PIL WP (C) 7483 of 2020*, 25 January 2021	The Court partially upheld the claim: - accepting the assurance given by the Government of India that the benefits of any services that are provided by the Governments, its agencies and instrumentalities is not denied to an individual on the ground that she has not downloaded and installed the contact tracing app. Moreover, the Court: - stating that the use and retention of information and data shall remain confined to what is provided in the privacy policy which is available on the contact-tracing app; - restraining the Government of India and the National Informatics Centre, respectively from sharing the response data by applying the provisions of the contact Data Access and Knowledge Sharing Protocol (2020), unless the informed consent of the app users is taken.	
France, Council of State, no. 44493, 13 October 2020,	The Council of State concluded that, even if it cannot be totally excluded, the risk that the US intelligence services will request access to the Health Data Hub, it does not justify, in the very short term, the suspension of the processing within the platform, but it does require special precautions to be taken, under the supervision of the French DPA.	
Israel, High Court of Justice, 2109/20 *Ben Meir v. Prime Minister*, 26 April 2020	- as the provision violates the basic right to privacy and considering the exceptionality of the COVID-19 crisis, the Court decided that as of April 30, 2020, it will not be possible to authorize the ISA to the data processing it was currently authorized. - A specific regime is designed by the Court for journalists (*the Ministry would ask a journalist who tests positive for the virus to consent to providing his details to the ISA. If*	Some prescriptions are directed to the defendant for the future.

	such consent is given, the mechanism would operate in the usual way. If the journalist refused, he will be granted 24 hours to petition the court for an order preventing the transfer of his data to the ISA. At the same time, he will undergo an individual epidemiological investigation, and will be asked to sign a declaration that he undertakes to inform any journalistic sources with whom he was in contact over the 14 days prior to his diagnosis.).	
Israel, High Court of Justice, 6732/20 *Association for Civil Rights in Israel v. Knesset*, 1 March 2021	The Supreme Court ruled that the government could not continue to authorize the ISA as a sweeping manner to assist in conducting epidemiological investigations.	
Spain, Supreme Court, no. 1112, 14 September 2021	The Supreme Court stated that the proposed measure must be authorised or ratified. The Court stated that the measure is proportional as the benefit provided by the measure (i.e., a significant reduction in contagions) is much greater than the sacrifice entailed by the requirement to present documentation for access to the premises. The Court took into account that there is no measure that would be more appropriate to safeguard the life and health of the public in such premises.	Ratification of a measure imposing limitations to fundamental rights.
France, Council of State, no. 440916, 19 June 2020	Lawfulness of the processing under the conditions that the Health Data Platform i) provide the French DPA with all information for enabling it to verify that the measures taken ensure sufficient protection and ii) will complete the information on its website relating to the project concerning the use of data on emergency room visits for the analysis of the use of care and the monitoring of the covid-19 health crisis in accordance.	Claim rejected under certain conditions for processing the defendant should ensure
India, Central Information Commission, *Saurav Das vs Deptt of Information Technology*, 26 November 2020	The complaint is rejected. The *Aarogya Setu* website needs to keep the information about the app up to date to be able to satisfy the citizens queries.	
India, The High Court of Orissa, Cuttack, *Ananga Kumar Otta v. Union Of India & Ors, WP (C)* No. 12430/2020, 16 July 2020	The Court rejected the claim, affirming that it hopes and trusts that: - the State shall take further steps if not already taken to keep the personal information masked by applying appropriate method, and keep utmost confidentiality of such information in intradepartmental communication. - that the Press shall behave in a more responsible manner with regard to disclosure of identity and should not disclose the identity of such persons unauthorizedly. Furthermore, *inter alia*, the Court stated that the State must have to vigil over spreading unauthorized information in the social media platforms and whenever it comes to their knowledge regarding such disclosure of names without authorization in the social platform, to legally proceed against such persons.	Claim rejected. Some prescriptions are directed to certain subjects
India, Madras High Court, *Adv. M.Zainul Abideen vs The Chief Secretary, W.P.No.7491 of 2020*, 22 April 2020	The Court dismissed the petition, affirming that it is not in the position to provide the guidelines to regulate the visual platform.	Claim rejected
India, High Court of Kerala, *Ramesh Chennithala vs State of Kerala*, 21 August 2020	Action dismissed	
Austria, Data protection authority, decision of 15 February 2021	The DPA stated that the transfer of results of a negative PCR test from a private medical center to public administration was lawful.	
Belgium, Council of State, Decision no. 248.124, 5 August 2020	Considering the guarantees for data processing, its regime and purpose, the Council of State held that the requirement of urgency required to suspend the contested act are not met, and accordingly rejected the claim.	
Belgium, Council of State, no. 248.108, 3 August 2020	The Council of State stated that the applicants' claims are based on provisions that do no longer have any effect in	

	the legal order or do not arise directly from the contested measure. Therefore, the Council held that the requirements of urgency required to suspend the contested act are not met, and accordingly rejected the claim.	
France, Council of State, no. 453505, 6 July 2021	The Council of State rejected the claims, considering that the implementation of the 'health pass' was not manifestly illegal at the date of its decision.	
France, Council of State, no. 450163 12 March 2021	The Council of State dismissed the request, noting that the data collected in the context of vaccination appointments did not include health data on the medical grounds for eligibility for vaccination and that guarantees had been put in place to deal with a possible request for access by the US authorities.	
Switzerland, Administrative Court of Zürich, AN.2020.00012, 3 December 2020	The Administrative Court rejected the claim, affirming that the measure establishing the obligation for accommodation and catering services to collect data of their guest for contact tracing purposes is proportional. The Court held that contact tracing is crucial for facing the COVID-19 crisis, according to scientific knowledge. The judges took into account several characteristics of the processing, such as the strict retention period and the fact that data can be processed only for contact tracing purposes.	
Colombia, Constitutional Court, judgement C-150/20, 27 May 2020	The provision under examination complies with the principles of freedom, purpose, necessity, confidentiality and restricted circulation. Therefore, that provision respects the standard of protection defined by constitutional jurisprudence for the effective guarantee of the fundamental right to *habeas data*.	Constitutionality of the measure

As shown by the table above, Courts or DPAs sometimes simply rejected the claim. In other cases, Courts and DPAs upheld, at least partially, the claim, providing the following remedies, obviously partially depending on the plaintiff's claims and on the type of procedure:

i) Declaration of unconstitutionality of the provision challenged

Constitutional Courts declared that the challenged measures contrasted with the Constitution for the lack of formal requirements or due to the violation of the right to private life, as the measure did not strike a fair balance between this right and the public health protection interests. In one case, the French Council declared the measure only partially in contrast with the Constitution.[154]

ii) Ratification/rejection of ratification

In Spain, some decisions concern the ratification of measures that limits fundamental rights. In one case, the Court affirmed the need to ratify the measure; in two cases judges rejected the ratification of the measures, as they were considered not proportional.

iii) Prohibition of processing (temporary or not)

In four cases the remedy was the prohibition of processing, sometimes temporary. The Brazilian case is quite different from the others, as the prohibition of processing is the consequence of the suspension of a provision enabling a specific processing, within a proceeding of constitutionality review of the measure.

iv) Courts' prescriptions about data processing

Sometimes Courts gave prescriptions regarding data processing, for example concerning data subjects' information[155] or data anonymization.[156] The decisions vary: in some cases, Courts upheld the claim[157], while in a case the claim was rejected

[154] French Constitutional Council decision no. 2020/800 of 21 May 2020154.

[155] French Council of State, dec. no. 440916 of 19 June 2020.

[156] High Court of Kerala, *Balu Gopalakrishnan & Anr. v. State of Kerala & Ors.*, W.P. (C). Temp No. 84, 24 April 2020.

[157] See French Council of State, 13 October 2020, n°, 44493; High Court of Kerala, *Balu Gopalakrishnan & Anr. v. State of Kerala & Ors.*, W.P. (C). Temp No. 84, 24 April 2020.

on condition that the defendant ensures certain information duties, *vis-à-vis* the national data protection authority and the data subjects.[158] Moreover, in two cases some prescriptions are directed to the defendant for the future.[159] Lastly, the case decided by the Polish data protection authority is quite different: the DPA ascertained the existence of a data breach and affirmed that the data controller is obliged to notify the data subjects of the breach without undue delay.[160]

In sum, when deciding on cases related to data protection rights during the current pandemic, Courts and DPAs applied a variety of existing data protection remedies. Courts' conclusions vary with regard to remedies and their impact on data processing operations, due to several factors, including the ones related to the type of action sought and to differences among legal systems.[161] However, the analyzed case law suggests that sometimes remedies are not only the outcome of the balancing between different interests (often protected as fundamental rights) but also a part of such balancing, at least where they encompass prescriptions adapted to the concrete case (e.g., the court's decision to give some prescriptions about the way data processing must be carried out and to not prohibit the processing may be interpreted as a balancing technique).

7. Insights from the Case Law Analysis

The case law analysis shows the importance of litigation in cases where personal data processing is directly aimed at addressing the ongoing pandemic. With regard to the legal issues addressed by Courts and DPAs, within data protection case law, as in other areas, crucial issues concern the balancing of different interests – often protected in the form of fundamental rights – and the remedies. Processing of personal data may be useful or necessary to face the current pandemic crisis (*e.g.*, contact tracing to limit contagions; management of vaccine appointments), while at the same time it shows the need of protecting data subjects' interests, not only related to privacy. For instance, there is the need to avoid discrimination against virus-positive individuals and, at least in respect to contact tracing, the risks of widespread surveillance.

Moreover, other interests and fundamental rights, such as freedom of expression, may be relevant.

The issue of defining the boundaries of lawful processing of data, ensuring both the protection of personal data and privacy and other fundamental rights or public and collective interests may be subject to further litigation, also challenging the notion of personal data itself.

In this respect, looking at the case law, the use and the public disclosure of aggregated data was at stake in an Indian decision, not subject of direct analysis in this article as Courts' arguments are not strictly related to data protection issues.[162] In this respect, the question of whether aggregated data are to be considered personal data may arise.[163] Moreover, the academic debate and case law may also concern the ways of balancing the right to data protection with the right to be informed.

Furthermore, the correct use of data for the purposes of scientific research, to ensure the reliability of the results is at stake in a decision of the Brazilian Federal Court of Accounts, not analysed in this paper because not strictly related to data protection aspects[164]. In this regard, the necessity to ensure both the reliability of scientific

[158] French Council of State dec. no. 440916 of 19 June 2020158.

[159] Israeli High Court of Justice, dec. 2109/20 *Ben Meir v. Prime Minister*, April 26, 2020; dec. 6732/20 *Association for Civil Rights in Israel v. Knesset*, March 1st, 2021.

[160] Decision of 12 November 2020, no. DKN.5101. 25.2020.

[161] In this respect, see the opening article of this section Fabrizio Cafaggi, Paola Iamiceli, 'Global Pandemic and the role of courts'.

[162] High Court of Delhi, *Vinay Jaidka v. Chief Secretary W.P.(C)* 5026/2021 & *CM APPL.* 15401/2021, April 28th, 2021.

[163] For example, in Europe according to art. 4 para. 1 no. 1 of the GDPR 'personal data' means any information relating to an identified or identifiable natural person, and an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. The case law of the Court of Justice of the EU addressed the notion of personal data on several occasions. In relation to the identifiability concept it is of particular interest *Breyer*, C-582/14, 19 October 2016; on this case see Frederik Zuiderveen Borgesius, 'The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition' (2017) Eur. Data Protection L. rev., 3, 130; Paul de Hert, 'Data Protection's Future without Democratic Bright Line rules. Co-Existing with technologies in Europe after Breyer' (2017) Eur. Data Protection L. rev. 1, 20. On the notion of personal data in the EU see also Nadezhda Purtova, 'The law of everything. Broad concept of personal data and future of EU data protection law' (2018) L. Inn. tech. 1, 40; Chiara Angiolini 'Lo statuto dei dati personali. Uno studio a partire dalla nozione di bene' (Giappichelli, 2020) 26.

[164] An English summary of the decisions is available at: <https://edpb.europa.eu/news/national-news/2020/temporary-suspension-norwegian-covid-19-contact-tracing-app_en> last accessed: 30 April 2021.

research and the respect of data protection and privacy rights could raise some legal questions related to possible conflicts (*e.g*., the publication of personal data is useful for allowing a control on the research outputs but could be detrimental for data subjects) or complementaries (*e.g.*, the control of data correctness and their periodic update) between the two interests at stake, which may be the subject of future litigation and research.

The analysis shows that often the necessity and the proportionality of processing for facing the COVID-19 crisis (e.g., through an effective contact tracing) are considered important criteria in the courts' and DPA's assessments. This analysis suggests that further litigation may concern the evaluation of necessity and proportionality in case of changes within the pandemic context. For instance, in case of improving health situation, may a judge consider data processing operations - that were lawful in a scenario worse than the current one - no longer necessary or proportionate, and, accordingly, consider that the balance struck between protection of public health and data subjects' rights is no longer correct? Which will be the role of scientific evidence in that regard? For instance, if the scientific knowledge concerning the Covid-19 will significantly evolve, may a judge rely on these scientific developments in conducting the proportionality and the necessity tests? If yes, how? Furthermore, in deciding concrete cases, Courts took into account the way data is processed, considering several factors (*e.g.*, the means, the data retention period, the category of data processed, the level of confidentiality). As an example, the possibility to adopt alternative solutions, less intrusive to the one in place is considered in certain cases as an important element. In this vein, in assessing the lawfulness of processing and in granting remedies, could Courts consider the effort (from an economic and technological point of view) made by people who conduct the processing (*e.g.,* public authorities) in developing and building less intrusive means for processing? Moreover, considering the possible use of AI tools for remote diagnosis within pandemic[165], may the elements considered in Section 4 be useful in order to assess the balancing between different interests (*e.g.*, infection risk of medical staff, data subjects' rights, patients' rights) with regard to these means of processing?

Moreover, looking forward, in relation to the use of "COVID certificates" or "COVID passports" several data protection issues may be subject of case law in the field of data protection. As showed by the existing case law, the principle of necessity in that regard could play quite a strong role: which are the categories of data, the retention period, the subject who can process such data, necessary for processing? The evaluation of scientific knowledge may also play a strong role in assessing the necessity and the proportionality of such measures, for example with regard to the assessment concerning the usefulness and necessity of such data for demonstrating a lower level of public health risk (e.g., immunity).

Moreover, the analysis shows the variety of remedies Courts adopted; such remedies have a different impact on data processing, from its ban to prescriptions concerning certain specific aspects of processing operations. The criteria Courts adopt (and should adopt) in selecting the remedy among the ones available, could be the subject of future litigation (*e.g.,* Courts may choice between temporary or permanent ban or the prohibition of certain means of processing).

8. Conclusion

This article has analyzed the case law collected within the COVID-19 Litigation project on personal data protection until November 2021. In particular, this survey focused on litigation concerning cases where the processing of personal data is directly aimed at addressing the ongoing pandemic.

The article firstly provides a very brief overview of the cases, focusing on the purposes of processing (Section 2). Then, the decisions are described in relation to the legal issues they address: the grounds for the processing of public interest and consent (Section 3), the different aspects of personal data processing that have been considered by the Court (Section 4), data transfers outside external borders (Section 5), and the remedies that courts have granted in individual cases, building a classification of those remedies (Section 6). A bottom-up approach was adopted for identifying the most important aspect of data processing considered by Courts in their reasoning and in classifying the remedies Courts granted. In the course of the analysis, as well as in Section 7, case law trends are critically considered, also looking at future litigation and possible lines of research to be further developed.

[165] See, for example, Marco Almada, Juliano Maranhão 'Voice-based diagnosis of COVID-19: ethical and legal challenges' (2021) International Data Privacy Law 11, 1. 63.

APPENDIX

TABLE OF CASES

DECISION	MAIN LEGAL ISSUES AT STAKE
Asia	
India, High Court of Kerala, *Balu Gopalakrishnan & Anr. v. State of Kerala & Ors., W.P. (C). Temp No. 84,* 24 April 2020[166]	Lawfulness of a contract between the Government of Kerala and a USA-based software company, aimed at creating an online data platform for data analysis of medical/ health data in relation to COVID-19 Data concerned: data concerning patients or persons susceptible to COVID-19 Nature of the parties: private and public (including the State of Kerala and the USA-based company).
India, Central Information Commission, *Saurav Das vs Deptt of Information Technology,* 26 November 2020[167]	Lack of transparency of the procedure of creation of a contact tracing app (*Aarogya Setu*), and on the related measures concerning the risk assessment of data processing and the security of the app. Data concerned: data processed through an app Nature of the parties: private (plaintiff); public body (defendants).
India, High Court of Kerala, *Ramesh Chennithala vs State of Kerala*, 21 August 2020[168]	Alleged violation of right to privacy (Art. 21 Constitutional law of India) through the collection of Call Detail Records by the police to track where the patients were prior 14 days before they were confirmed to be positive. Data concerned: Call Detail Records (CDRs) Nature of the parties: an individual who is member of the Legislative Assembly (plaintiff), public body (defendant).
India, Madras High Court, *Adv. M. Zainul Abideen vs The Chief Secretary, W.P.No.7491* of 2020, 22 April 2020[169]	Request for guidelines concerning the media broadcasting visual news of confirmed Covid-19 patients with specific religion Data concerned: identity of Covid-19 patient with specific religion Nature of the parties: private (plaintiff); public body (defendants).
India, The High Court of Orissa, Cuttack, *Ananga Kumar Otta v. Union of India & Ors., WP (C) No. 12430/2020*, decisions of 28 May 2020 and of 16 July 2020	Compatibility of the disclosure of the identity of the confirmed Covid patients with the right to privacy Data concerned: identity of Covid patients Nature of the parties: private party (plaintiff); public body (defendant)
India, High court of Karnataka, *Anivar A Aravind v. Ministry of Home Affairs, GM PIL WP (C) 7483 of 2020*, 25 January 2021	Assessment of the some aspects aspects of a contact-tracing app, including its mandatory caracter for accessing certain services and the existence of the data subcjects' consent to data processing. Data concerned: health data, location data, contact details, sex, profession Nature of the parties: private party (plaintiff); public body (defendant)
Israel, High Court of Justice, 2109/20 *Ben Meir v. Prime Minister*, 26 April 2020[170] °	Legitimacy of a Government decision providing the Israel Security Agency (ISA), to process, for purposes of contact tracing and control over the respect of COVID-19 measures, "technological information" regarding persons who tested positive to COVID-19, as well as persons who came into close contact with them. The provision applied to journalists as well. Data concerned: "technological information" for identifying the route of the movement of anyone who tested positive for the virus during the 14 days prior to the diagnosis, and location data concerning all the people who were in that person's close proximity for more than a quarter of an hour. Nature of the parties: Associations, individual (plaintiffs); public bodies (defendants)
Israel, High Court of Justice, 6732/20 *Association for Civil Rights in Israel v. Knesset*, 1 March 2021	Lawfulness of a Government decision enabling the Israel Security Agency to use tracking technological means for epidemiological purposes regarding persons who had tested positive to the COVID-19, as well as contact persons.

[166] The decision is available at: <https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2020/05/Balu-gopalakrishnan-v-State-of-kerala.pdf> accessed 5 May 2020.

[167] The decision is available within the database: <https://indiankanoon.org/> accessed 5 May 2021.

[168] The decision is available within the database: <https://indiankanoon.org/> accessed 5 May 2021.

[169] The decision is available within the database: <https://indiankanoon.org/> accessed 5 May 2021.

[170] The decision is available, in English, at: <https://versa.cardozo.yu.edu/opinions/ben-meir-v-prime-minister-0> accessed 5 May 2021.

	Data concerned: information concerning people who had tested positive for the novel coronavirus, as well as persons who came into close contact with them. Nature of the parties: Associations (plaintiffs); public bodies (defendants)
Europe	
Austria, Constitutional Court, V 573/2020, 10 March 2021	Constitutionality review of a provision establishing, for contact tracing purposes, that restaurant owners must collect personal data of customers and to transmit such data to the competent authorities if asked. Data concerned: data concerning restaurants' clients Nature of the parties: private party (plaintiff)
Austria, Data protection authority, Decision of 15 February 2021[171]	The lawfulness of an administrative act imposing a duty of private health centers to share negative results of PCR tests with public administration. Data concerned: data on the results of a PCR test for SARS CoV-2 from a primary care center Nature of the parties: private (plaintiff)
Belgium, Council of State, no. 248.124, 5 August 2020[172]	Urgency procedure for suspension against a ministerial order imposing, *inter alia*, the communication of personal data in catering establishments Data concerned: telephone number and e-mail address (limited to one for each group of clients sharing the same restaurant table). Nature of the parties: private parties (plaintiffs) and public body (defendant).
Belgium, Council of State, no. 248.108, 3 August 2020[173]	Urgency procedure for suspension against a ministerial order imposing, *inter alia*, the communication of personal data in catering establishments Data concerned: telephone number and e-mail address (limited to one for each group of clients sharing the same restaurant table). Nature of the parties: private parties (plaintiffs) and public body (defendant).
France, Council of State, no. 453505, 6 July 2021[174]	Procedure for the suspension of the use of the 'health pass' (QR Code requiring the processing of data relating to civil status and of health data) Nature of the parties: Data protection association (plaintiff); public body (defendant)
France, Council of State, no. 450163, 12 March 2021[175]	Lawfulness of data transfers to a third country, outside the European Economic Area (EEA) Data concerned: personal identification data and data relating to appointments (not health data) Nature of the parties: Associations and trade unions (plaintiff); public body and private company (defendant)
France, Council of State, no. 44493, 13 October 2020,[176]	Lawfulness of data transfers to a third country, outside the European Economic Area (EEA) Data concerned: health data Nature of the parties: associations and trade unions (plaintiff); public body (defendant)
France, Council of State, decision nn. 440442, 440445, 18 May 20220; Council of State, decision no. 446155, 22 December 2020[177]	Lawfulness of the processing of data through drones by the police, for purposes of surveillance of the compliance of health regulation in force during the COVID-19 emergency. Data concerned: personal data registered by drones Nature of the parties: Data protection association (plaintiff), public body (defendant)

[171] The author/s thanks M. Grochowski and O. Ceran for the help they provide for the understanding of the case.

[172] The decision is available, in French, at: <http://www.raadvst-consetat.be/arr.php?nr=248124> accessed 5 May 2021.

[173] The decision is available, in French at: <http://www.raadvst-consetat.be/arr.php?nr=248.108> accessed 9 December 2021.

[174] The decision is available, in French at: <https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2021-07-06/453505> accessed 5 May 2021. The Press release in English is available at: <https://www.conseil-etat.fr/en/news/the-conseil-d-etat-decides-not-to-suspend-france-s-health-pass> accessed 9 December 2021.

[175] The decision is available, in French, at: <https://www.legifrance.gouv.fr/ceta/id/CETATEXT000043261200 accessed> 5 May 2021.

[176] The decision is available, in French, at: <https://www.legifrance.gouv.fr/ceta/id/CETATEXT000042444915> accessed 5 May 2021.

[177] The decisions are available in French at: i) <https://www.conseil-etat.fr/ressources/decisions-contentieuses/dernieres-decisions-importantes/conseil-d-etat-18-mai-2020-surveillance-par-drones ; ii) <https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2020-12-22/446155> accessed 30 April 2021.

France, Council of State, no. 440916, 19 June 2020[178]	Lawfulness of data processing, within a platform of health data for facilitating the use of health data for improving the health emergency management and fostering knowledge about covid-19. Data concerned: health data Nature of the parties: Associations, professional associations, trade unions (plaintiffs); public body; representative of the 'Health Data Hub', a body constituted by public and private bodies (defendants)
France, Council of State, decision no. 441065, 26 June 2020[179]	Lawfulness of the processing of data through portable thermal imaging cameras used by municipal staff in schools to measure the body temperature of students, teachers and municipal staff working on school premises (data processing provided for by a municipal order). Data concerned: health data (temperature) Nature of the parties: fundamental rights' association (plaintiff); public body (defendant)
France, Constitutional Council no. 2020/800 21 May 2020[180]	Constitutional review of the compatibility of privacy right with a provision setting conditions under which the medical data of people infected with COVID-19 and those who have been in contact with them may be shared between certain professionals responsible for dealing with infection chains. Data concerned: health data Nature of the parties: President of the Republic; President of Senate, individuals (plaintiffs)
Montenegro, Constitutional Court, U - II 22/20, 23 July 2020	Constitutionality review of the decision, taken by the National Coordinating Body for Contagious Diseases, to publish names and addresses of persons in self-isolation in relation to COVID-19 on the Government website Data concerned: names and addresses of persons in self-isolation in relation to COVID-19 Nature of the parties: private (NGO, plaintiff)
Norway, Data Protection Authority, decisions of 15 June and 17 August 2020[181]	Compatibility with the data protection legal framework of the contact tracing app developed by the Norwegian Institute of Public Health (NIPH), used for contact tracing purposes and for monitoring the pandemic. Data concerned: personal data about app users, including continuous location data (GPS) and information about app users' contact with others Nature of the parties: public body – sanctioning procedure
Poland, Data Protection Authority, no. DKN.5101.25.2020, 12 November 2020,[182]	Existence of confidentiality breach of data concerning addresses of persons subject to quarantine and related obligations of the data controller. Data concerned: list with addresses of persons quarantined based on the decision of the State Sanitary Inspector, persons quarantined following a return from abroad, and persons with active COVID-19 infection in obligatory domestic isolation Nature of the parties: public body (plaintiff)

[178] The decision is available in French at: <https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2020-06-19/440916> accessed 30 April 2021.

[179] The decision is available in French at: <https://www.conseil-etat.fr/ressources/decisions-contentieuses/dernieres-decisions-importantes/conseil-d-etat-26-juin-2020-cameras-thermiques-a-lisses> accessed 5 May 2021.

[180] The decision is available in French at: <https://www.conseil-constitutionnel.fr/sites/default/files/as/root/bank_mm/decisions/2020800dc/2020800dc.pdf> accessed 30 April 2021 (English and Spanish translations are provided).

[181] An English summary of the decisions is available at: <https://edpb.europa.eu/news/national-news/2020/temporary-suspension-norwegian-covid-19-contact-tracing-app_en> accessed 30 April 2021.

[182] The author/s thanks M. Grochowski and O. Ceran for the help they provide for the understanding of the case.

Spain, Supreme Court, no. 1112, 14 September 2021[183]	The decision concerns a procedure for ratification of health measures restrictive of fundamental rights. The measure at stake limited the access to certain inside entertainment establishments to those persons who can prove that they have a valid 'COVID passport' Data concerned: data included in the 'COVID passport' Nature of the parties: public body (plaintiff)
Spain, Supreme Court, no. 1103, 18 August 2021[184]	The decision concerns a procedure for ratification of health measures restrictive of fundamental rights. The measure at stake limited the access to inside entertainment and hospitality establishments with music to those persons who can prove that they have a valid EU Covid digital certificate or accreditation of antigen test or negative PCR in the last 72 hours carried out in health centres, services or establishments. Data concerned: data included in the EU Covid digital certificate or in the document concerning the antigen test or negative PCR. Nature of the parties: public body (plaintiff)
Spain, Asturias High Court of Justice, 10 June 2021[185]	The decision concerns a procedure for the ratification of health measures restrictive of fundamental rights. The measure at stake imposed the obligation for hotels and restaurants to draw up and retain for 30 days an attendance list and for nightlife establishments to draw up and retain for 30 days a list of clients. Data concerned: date and time of entry and exit of attendees or clients, their name and/or surname and their contact telephone number. Nature of the parties: public body (plaintiff)
Switzerland, Administrative Court of Zürich, AN.2020.00012, 3 December 2020[186]	The decision addresses the claim for the revocation of a regulation introducing the obligation for accommodation and catering services to collect data of their guests for contact tracing purposes. Data concerned: surname, first name, postcode, mobile phone number, e-mail address, time of entry and exit to the catering establishment Nature of the parties: private individual (plaintiff), public body (defendant)
South America	
Brazil, Federal Supreme Court ADI 6387 MC-REF decisions of 24 April and 7 May 2020[187]	Constitutionality review of provisions of the Provisional Presidential Decree 954/2020, which obliged telecommunication Companies to share the list of names, telephone numbers and addresses of their consumers with Brazilian Institute of Geography and Statistics Foundation, for supporting official statistic during the public health emergency resulting from the COVID-19 pandemic. Data concerned: list of names, telephone numbers and addresses of clients of telecommunication companies Nature of the parties: Brazilian Bar Association (plaintiff)
Colombia, Constitutional Court, judgement C-150/20, 27 May 2020	Constitutionality review of the Legislative Decree 458 of 2020, providing measures against poverty in the framework of the State of Economic, Social and Ecological Emergency. According to that measure, the National Administrative Department of Statistics shall provide the information collected in censuses, surveys, and administrative records to the State entities responsible for adopting measures for the control and mitigation

[183] The decision is available in Spanish at <https://www.poderjudicial.es/search/AN/openDocument/308a9176fc4b9502/20210920> accessed 10 December 2021.

[184] The decision is available in Spanish at : <https://www.poderjudicial.es/search/AN/openDocument/5774c96862c0f7ef/20210827 accessed 9 December 2021.

[185] The decision is available in Spanish at <https://www.poderjudicial.es/cgpj/es/Poder-Judicial/Tribunales-Superiores-de-Justicia/TSJ-Asturias/Noticias-Judiciales-TSJ-Asturias/El-TSJ-de-Asturias-no-ratifica-medidas-del--Gobierno-del-Principado-relativas-a-establecimientos-de-hosteleria-y-ocio-nocturno-> accessed 9 December 2021.

[186] The decision is available in German at: <https://vgrzh.djiktzh.ch/cgi-bin/nph-omniscgi.exe?OmnisPlatform=WINDOWS&WebServerUrl=https://vgrzh.djiktzh.ch&WebServerScript=/cgi-bin/nph-omniscgi.exe&OmnisLibrary=JURISWEB&OmnisClass=rtFindinfoWebHtmlService&OmnisServer=JURISWEB,127.0.0.1:7000&Parametername=WWW&Schema=ZH_VG_WEB&Source=&Aufruf=getMarkupDocument&cSprache=GER&nF30_KEY=220831&W10_KEY=5555488&nTrefferzeile=4&Template=standard/results/document.fiw> accessed 9 December 2021.

[187] The decision is available in Portughese at <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf> accessed 30 April 2021.

	of the COVID-19 coronavirus, when requested by them for the implementation of measures for the control and mitigation of the COVID-19 coronavirus. These data may only be used for that purpose. Data concerned: databases of the National Administrative Department of Statistics Nature of the parties: public bodies (constitutional review procedure), intervention by universities and private citizens