ARTICLE February 2024

ALBANIAN LAW JOURNAL

The Balance Between the Right to Information and the Right to Privacy in Judicial Decisions: The Case of Albania

Hysmir Idrizi LL.M
Gentiana Kapllani LL.M

Funded by the European Union

ALBANIA Law Journal

EUROPEAN MOVEMENT ALBANIA

PUBLISHER

European Movement Albania (EMA)
Rr. Milto Tutulani, Nd. 1, Ap. 4 (Dora D'Istria)
Tirana 1019, Albania
Tel: +355 44 104 247
E-mail: info@em-al.org
Web: www.em-al.org

AUTHORS

Hysmir Idrizi LL.M
Gentiana Kapllani LL.M

YEAR OF PUBLICATION

February 2024

Hysmir Idrizi, LL.M., has a solid background in International and Commercial Law. Holding a Master of Laws degree from the University of New York Tirana, Hysmir is also equipped with a Diploma in Collaborative Governance in a Digital Era from the Swedish Institute Academy for Young Professionals. Currently serving as the Office Coordinator for the CleanScore Project at the Albanian-American Development Foundation, Hysmir oversees project implementation and strategic plans. Hysmir has pursued additional certifications, including Collaborative Governance, Principles and Purposes of Assessment, and GDPR Compliance.

With a Bachelor's degree in Law from the University of Tirana and an LL.M. from the University of New York in Tirana, Gentiana Kapllani has honed her expertise in legal writing, research, legal-tech, startups, entrepreneurship, marketing, and public relations. Currently serving as the Office Coordinator for the CleanScore project at the Albanian-American Development Foundation, Gentiana is responsible for project implementation at the Polytechnic University of Tirana. She has a track record of active participation in various organizations and in research activities.

This publication was funded by the European Union. Its contents are the sole responsibility of European Movement Albania, Albanian Law Journal and its authors and do not necessarily reflect the views of the European Union.

The action "Building Partnership on Fundamentals: Empowering CSOs for the EU accession process", is being implemented by the European Movement in Albania, with the financial support of the European Union - IPA Civil Society Facility 2021, and in cooperation with the Academy of European Integration and Negotiations (AIEN), Slovak Foreign Policy Association (SFPA) and the Center for Transparency and Freedom of Information (CTFI).

Funded by the European Union

ALBANIA Law Journal

EUROPEAN MOVEMENT ALBANIA

Three major revolutions have shaped and reshaped the way society cooperates as a whole entity: the Agricultural Revolution, the Industrial Revolution, and the Technological Revolution.[1] Started in 1970 with the emergence of new technologies, the latter paved the way to a novel way of social interaction, the one that is referred to today as “the information society”. Each subject - whether a physical or a legal entity - is a load of data to information and communication technologies, the protection of its rights has become an offset for immense legal amendments.[2] Considering this, this paper outlines two of the most affected rights by technological development - ‘the right to information’ and ‘the right to data protection’.

This paper outlines a new approach to maintaining a balance between the protection of personal data and the right to information in legal proceedings. In the first section it provides a general introduction of the standards set by the “General Data Protection Regulation" by considering different ‘minimisation techniques’ applied by the European Member States as applicable approaches for a better protection of personal data in legal proceedings. In the second section it analyzes the protection of these rights in Albanian legislation and proposes possible solutions to be implemented by the courts and the Public Relations Offices - as the responsible institutions according to the law. It considers legal doctrine, as well as the Xhoxhaj vs. Albania, a case law directly addressing the level of personal data protection that should be guaranteed by the State. In conclusion, the paper underlines the importance that the ‘test of proportionality’ has for safeguarding citizens’ rights in a society with unprecedented technological advancements.

The right to information

From the Great Age of Reason to modern democracies, the right to information bears an exceptional role in the well-functioning of societies and the enjoyment of other human rights.[3] Citizens' capability to be informed on the government's public works and State's activity is crucial for a functional democracy, but it has not always been like this. Whereas the right to information has been indicated as a basic human right in various international agreements and protected as such by several international guarding structures of human rights [4], at an EU level - it was granted explicit protection only in 2009, when the Council of Europe (CoE) signed the "Convention on Access to Official Documents".[5] Even though this Convention entered into force years later, in December 2020, it has a preeminent role in its obligatory nature. It is the first binding international agreement that acknowledges the right to access official documents carried by public authorities.[6]

Article 2 of the Convention gives a definition of the right to information and charges the responsibility of all public authorities to comply with its legal requirements. As defined in the first paragraph of Article 2, once the Convention is ratified, "each Party shall guarantee the right of everyone, without discrimination on any ground, to have access, on request, to official documents held by public authorities."[7]

The Albanian State is one of the parties to this Convention. Therefore, the administrative and judicial authorities shall guarantee such a right. Natural or legal persons when exercising public functions shall be constrained to this requirement. Whereas the Albanian State, as stipulated in the second paragraph of the Convention, shall "take the necessary measures in its domestic law to give effect to the provisions for access to official documents."[8] As outlined, the right to information is considered as a "fundamental human right" in nearly all national constitutions and international treaties.[9] Consequently, all public and private actors in these signatory States shall actively engage in the protection of such rights. However, the reality is quite convoluted, especially in this time of big data. [10]

Throughout the years, the right to information has been subject to legal restrictions.[11] Influenced by technological developments and society's perceptions of public claims, the legal right to information is altered for the protection of another right, the right to data protection. General Data Protection Regulation (GDPR) is the utmost example of this level of protection. GDPR is an extra-territorial binding Regulation, meaning that it finds application outside the borders of the EU regardless of the physical place where the data processing is taking place. For instance, a data processor based in England shall apply a data processing policy in compliance with the requirements of the GDPR for the same data processing processes that take place both in England and Italy.[12] Thus, this controller guarantees at the same time legal protection to the gathered data and avoids entitlements to vigorous fines.[13]

General Data Protection Regulation (GDPR): a New Standard

The most important international document on data protection is the the Regulation No. 2016/679, The General Data Protection Regulation (GDPR) [14], approved by the European Parliament in 2016. [15] Before the present Regulation, the governing legal instrument regulating data protection in the European Union (EU) was the Data Protection Directive (Directive 95/46/EC). It was enacted in 1995 and replaced in 2018, supervening the recommendations of the Data Protection Working Party (WP) [16] for improved and comprehensive data protection. GDPR reflects the recommendations of the WP and provides a new and strengthened approach to data protection at the EU and international levels. [17] GDPR's imperative prominence lies in the new standard it set for comprehensive data protection, despite the factual location of the data subject or the data controller and served also as a legal model for other jurisdictions in the world. [18]

The protection of personal data constitutes the foundation of this Regulation. GDPR defines 'personal data' as: "any information relating to an identified or identifiable natural person. Under this definition, the GDPR sets out the condition that only the natural person ("data subject") can be entitled to the legal protection guaranteed by this regulation. Moreover, the same article[19] stipulates that "the 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."

From this definition, we can come to the point that information such as name, identification number, physical features, health condition, cultural and socio-economic status, online identifiers, and location data - are all data that can make a person identifiable. To that end, in the physical and legal areas where the GDPR is in force, all data that make a person identifiable shall be minimized. [20]

Data Minimisation

GDPR finds application only to personal data which has the potential to make the natural person identifiable. This is specifically expressed in the recital 26 of the Regulation, as the following: "The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable." [21] In this line of thought, in conditions when the potential identifiable information of a natural person is anonymous, the natural person becomes unidentifiable. Consequently, there is no space for GDPR application once data minimization happens.

Specialists in the field of Information Technology use different minimization techniques to make data identifiable. Minimization is an umbrella term for

anonymization, unlikability, minimization, observability, and pseudonymization - applied by Privacy Enhancing Technologies (PETs). The purpose of all these techniques lies in three fundamental actions. First, on the circumstances for collecting personal information from data subjects. They shall be limited.

Secondly, on the application of any minimization technique. After data have been mined and explored, they shall be minimized. And thirdly, on the correlation time period-data storage. The time period data are stored shall be as little as possible.[22] Then again, with a GDPR that doesn't impose any requirement for anonymization, but only requires data minimization - which is limited data usage for the purpose data is collected [23] - private and public actors shall align their data processing activity to the provisions of their national laws. The only minimization technique specified in the GDPR is "pseudonymization". Under this technique, data is minimized by identifying a person with a pseudonym which makes it impossible for his identification. [24] The best practice of data minimization comes from the EU member states, which have implemented the GDPR and its standards in harmony with the nature of their domestic legislation.

Minimization and Data Protection

Any information in documents put on the web can be read in two forms: manually - by humans (1), and digitally - by machines (2). When a court decision is published online, it guarantees the fulfillment of several fundamental rights: citizens' right to information, welladministration of justice, and transparency in decision-making.[25] On the other hand, with the GDPR in force, convenient importance should be given to the protection of the personal data of the parties involved in litigation processes.

The application of an appropriate minimization technique for data protection is what matters on behalf of data protection.[26] Minimization might be a legal requirement, but not a 'one-size-fits-all it all' standard. To that end, they might be applied in different techniques. The working group of euro experts have advised the same when framing the guidelines for a convenient application of the minimization technique. To that end, minimization might be practiced either by diminishing in initials the name of the parties involved and other personal data belonging to them, such as the ID number or home address, or by following the best practices of other member states - which have altered and applied different minimisation methods.[27]

Right after the GDPR entered into force, the best example of minimisation technique application comes from the Court of Justice of the European Union (CJEU). In order to comply with requirements of the Regulation on data protection in the publications of court's decision - the court publicly issued an administrative decision expressing that: "in all requests for preliminary rulings brought after 1 July 2018, the court is to replace, in all its public documents, the name of natural persons involved in the case by initials. Similarly, any additional element likely to permit identification of the persons concerned will be

removed." By applying the anonymization technique, moreover, the Court stated that: "when the case is between only natural persons, the case name will correspond to two initials representing the first name and surname of the applicant, but different from the true name and surname of that party."[28] From here we can see not only the application of anonymisation but data replacement using other initials.

"Anonymization" and "minimization" techniques are two important mechanisms which, if used accordingly, safeguard at the same time - the protection of the right to information and the right to privacy. The "anonymization" technique is not applied one and the same in all Member States. In certain jurisdictions it is administered as a rule, in others as an exception to the rule, and to some other ones - to a certain degree.

In those States where anonymization is required by law [29], all court decisions are anonymised on publication, despite the court's tire. This is the case of Germany, Hungary and Greece, among others.[30] When anonymization is an exception to the rule, courts are not obliged to follow up with this technique, unless the decision contains sensitive information relating to the parties involved.[31] In Cypriot, Irish, Italian, Maltese and United Kingdom legal orders, anonymisation is applied as an exception to the rule. Whereas, in those jurisdictions where anonymization is applied to a certain degree - not all courts of all levels are obliged to follow this technique.[32] The Croatian, Spanish, French, Latvian, Lithuanian, Polish, Romanian, Slovenian and Czech high courts are obliged to apply the anonymization technique to a certain degree. Notwithstanding, anonymization is not uniform per se.

In some States, courts disclose all together with the decision, only the initials of the physical person.[33] That is the case of German, Belgian and Italian legal orders, among others. And, when one of the parties is a minor, some legal orders - such as the one in the United Kingdom - require the initials to be put next to the denomination 'the child'.[34] Wherever parties are asylum seekers, the name of a physical person shall be replaced by his initials and the state of origin. This practice is applied in the United Kingdom and Slovenia.[35]

Delving into the anonymization technique, we can come to the conclusion that from jurisdiction to jurisdiction it finds different applications, based on the status of the physical person, the category of the court, the data type and the type of court decision. At times, in certain jurisdictions, only the electronic format of the court decision is anonymized when published. In any case, parties' right to information prevails. Regardless of which minimization technique the court applies, parties have always the right to have access to the full form of the decision. On this occasion, the right to information equals the right to data protection.

Overall it might be said that the necessity for a comprehensive data protection has introduced formal restrictions to the right and access to information. Once the GDPR entered into force, it affected international treaties and national laws.[36] European member states adjusted their domestic legislation in accordance with the requirements of GDPR by applying different minimisation techniques, to guarantee a balance between two seemingly conflicting rights: the right to information and the right to have protected personal data.

The Albanian State has implemented imminent legal amendments in its domestic legislation. In particular regarding the protection of personal data in legal proceedings as analyzed in the second section of this paper.

Albanian Legislation: The Right to Information v. Right to Privacy - Managing Conflicts and Finding Balance

This section analyzes how the court finds the balance between the right to information and the right to privacy in case of conflict, throughout the activity and exercise of its judicial functions. The right to a private life is one of the fundamental human rights that underlie the entire legal system, as part of the protection of the dignity and development of the human personality, which can grow and develop mainly in a private environment.[37] However, the court as a public authority,[38] in addition to protecting these rights, is also responsible for fulfilling constitutional obligations such as the obligation to conduct a public, fair, and impartial trial within a reasonable time.[39] The public, on the other hand, has the right to be informed, without explaining the motives, about the activity of the court.[40]

As the court performs its duties, it adheres to the principles of accountability and transparency. It strives to keep the public informed about its activities, the cases it has judged, and those still under review. Additionally, it ensures that its decisions are well-reasoned and published. Every individual has the constitutional right to be informed about the activities of public authorities, , including the court. This ensures transparency and accountability. The court is a public authority responsible for delivering justice. As part of its duties, it must take measures to protect fundamental rights and freedoms, and ensure they are upheld.[41] It can be challenging for the court to balance the need for transparency on one hand, and protection of privacy rights on the other hand. However, the court needs to perform its obligation to inform the public while also safeguarding individual rights. By doing so, the court can ensure that justice is delivered fairly and in accordance with the law.

This article emphasizes the importance of the principle of due process of law (fair trial – Article 6 ECHR), which must be upheld by the judicial bodies to carry out their duties effectively. The European Convention on Human Rights (ECHR) defines the due process of law as follows: “In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interests of morals, public order, or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice."[42]

The court hearings are generally public unless national interests, security, public order, morals, protection of minors, or private life of parties are at stake, or if the interests of justice would be compromised.[43]

A public hearing cannot be held solely based on public interest without considering the test of proportionality when it comes to rights such as the right to privacy.

The court is obliged to provide the public with information about its activities and establish a transparency program[44] to increase accountability and transparency. Nonetheless, the legitimacy of the court derives not only from the law but also from performing its obligation to be transparent and accountable to the public. Even in closed proceedings sessions, decisions must be made public.[45] The objective is not to disclose the identity of individuals involved in a case, but rather to comprehend how the court has employed and construed the law. Thus, the obligation that "judgments must be made public, but access to the courtroom may be restricted for the press and the public throughout the entire process or a portion of it"[46] is directed to the court as a public body, rather than the litigants or parties involved.

The public has the right to access information that is produced or held by public authorities, which promotes integrity, transparency, and accountability.[47] This is essential for strengthening democratic and institutional governance.[48] It also helps people understand how the judicial system works and how justice is delivered. Consequently, the public can adopt a critical approach to compare the presumed constitutional situation with the current reality. This can result in increased demands for accountability and transparency from judicial authorities. The protection of personal data is important for respecting human rights and preserving privacy, preventing illegal and unjustified interference by public authorities. Limits on fundamental rights and freedoms can only be imposed through the law and must not exceed the limits set by the European Convention on Human Rights.[49]

Personal data is any information that can identify an individual and is categorized into general, judicial, and sensitive data. The objective of the law on protection of personal data is to guarantee a fair and legal processing of personal data while ensuring the protection of fundamental human rights and in particular, right to privacy.[50] General data information is unique and reveals the person's physical, social, cultural, economic, or mental identity. [51] Judicial data pertains to information about criminal, administrative, or civil decisions, as well as any documented data in civil, administrative, or criminal records. Sensitive data also includes information about criminal convictions.[52] The concern is whether releasing this data could infringe on the individual's private life, freedom to choose their lifestyle after serving their sentence, and the risk of being stigmatized.[53] Such stigmatization may harm their right to earn a living with dignity.

The Constitution of the Republic of Albania provides individuals with the fundamental right to keep their personal data private unless the law permits its disclosure.[54] Even without obtaining the subject's prior consent, data related to individuals may be processed and published in certain circumstances outlined by law. However, the law must have a specific purpose to justify such restrictions on privacy. For instance, officials' and public servants' data

may be published, limiting their right to privacy due to their public function. The law must prioritize public interest over fundamental rights and freedoms. The court must follow the principles of legality, proportionality, and data collection purpose[55] while exercising its constitutional functions. Moreover, the court must also take appropriate measures to protect against unjust infringement and unjust interference in private life. Data processing for scientific purposes[56] also falls under these rules, and the subjects' identities cannot be published or used. In other cases, the data subject's consent is required.

The Constitutional Court has defined the right to information as a critical aspect of democracy and an essential tool for controlling the government's actions.[57] Therefore, the right to information increases transparency and accountability for public authorities, including the court.

When two rights conflict, the Constitutional Court states that the court must consider the intensity and degree of violation of private life, the necessity of intervention in a democratic society, the effectiveness and proportionality of the interference, and whether the litigant is exempt from the obligation to publish personal data. If the litigant is not exempt, the court must also consider whether publishing the identifying information serves justice.[58] The Xhoxhaj vs. Albania case is an example of an exceptional case where personal data must be made public. The European Court of Human Rights (ECtHR) ruled based on Article 8 of the ECHR, which recognizes the right to private and family life but allows limitations defined by law. The right to information is part of public interests, while the right to private life is part of individual rights and freedoms. The former is directed toward public authorities to publish their activity related to law implementation and interpretation, while the latter requires protection and appropriate measures from public bodies.

The case of Xhoxhaj v. Albania was reviewed by the European Court of Human Rights (ECtHR) to determine if there was a breach of the right to privacy due to dismissal from office, and if the breach was connected to any of the cases outlined in Article 8 of the ECHR. Firstly, the ECtHR examined if the dismissal was based on law no. 84/2016 "The transitional re-evaluation of judges and prosecutors in the Republic of Albania", which was previously upheld by the Constitutional Court.[59] The ECHR found no breach of Article 8 in this regard. Secondly, the ECtHR assessed the necessity of the dismissal regarding a democratic society. It was determined that any interference with the right to privacy must be justified by a purpose that aligns with the set goals in Article 8 and is necessary for a democratic society. The law in question aimed to combat corruption and restore public trust in the judiciary system.[60] The ECtHR concluded that dismissal is a severe disciplinary action that should only be taken if there is consistent evidence regarding the individual's ethics, integrity, and professional ability.[61] Consequently, the case of public officials and servants is an assessment of the balance between the right to information and personal data protection under Article 8 of ECHR. Public officials have accepted that their position is not the same as private parties, but their privacy cannot be violated unless it is in the public interest.[62] The publication of data and dismissal, in this case, was justified by the public nature of the function, but each case

must be evaluated individually based on the ECtHR's jurisprudence.

To sum up, the test of proportionality must be assessed in the context of fundamental rights and freedoms in conjunction and in accordance with public law. The personal data of the subject will be published only in cases where their publication does not threaten the rights and legitimate interests of the subject to which they belong.[63] In any case of publication, the court is obliged to place the initials of the parties or to codify the parts that contain personal or sensitive data.[64] However, even though at first sight, these rights may seem to protect two objects that are opposite to each other, this cannot be understood only in this way, but also as complementary, because although their object is different but not necessarily opposite. However, the limitation of fundamental rights and freedoms only by law serves as a guarantee for the holders of these rights, in order not to subject you to illegal actions of public authorities. The threshold of this restriction cannot in any case exceed the threshold established by the ECHR.

The Relationship between Court and the Public: the right to information vs the right to privacy

This section examines the criteria for determining which information falls under unrestricted access and which falls under limited access. The purpose of regulating the court's relationship with the public is to determine the court's responsibilities in ensuring the public's right to information. The court must perform this task in a fair and within a reasonable time.[65] To aid in this effort, the court should have a Public Relations Office (PRO) responsible for creating press statements that inform the public about specific cases or trial activities, even when not requested by the public. The PRO can advise the judge or the judicial panel on the advantages and disadvantages of taking a public stance.[66] To do so, the PRO must have qualified personnel and experts in communication and public information, with relevant training in fundamental human rights and freedoms with a very narrow training on the right to information and privacy.

The court is obligated to inform the public through various means of communication and information, including its website, which should be updated regularly with information related to its activities.[67] As the controller of personal data in its activity, the court is authorized to process and control personal data within the framework of the exercise of its constitutional function, with limitations to protect basic human rights and freedoms, including the right to privacy.[68] When publishing court decisions online, the court must consider anonymizing the identities of parties, third parties, witnesses, and experts by using initials or codes.[69] This measure is designed to protect identities and maintain privacy. The court is required to publish certain decisions, such as commercial or family legal disputes while anonymizing the identities of juveniles.[70] The court's press release related to a case should include the session date, time, and location, the general circumstances of the trial, and the court's interim or final decision.[71] The statement should be written in simple and easy-to-understand language, without including statements from witnesses, judges, experts, prosecutors, or other parties.[72]

Regulation no. 6777/5 on "Court's Relationship with the Public" is crucial in defining the rules for information disclosure by the court. It lays out what information should be freely available to the public and what information should be restricted.[73] First, courts must provide unrestricted access to all court decisions at every level of trial.[74] This is in accordance with the obligation that a court's decision must be public in any case, regardless of whether the court hearings were held private.[75] However, there is a contrast noted within this regulation between the definitions of information with unlimited and limited access. Point 3.4 of the regulation provides information related to civil lawsuits, the parties involved, and the object of the lawsuit, under the category of information with unlimited access. Meanwhile, point 5.1 lists the personal data of each person under the category of information with limited access, contradicting point 3.4 on the generalities of the parties in a civil trial. Contrarily, in judicial-administrative hearings, the regulation foresees that the identity of the parties involved in the trial will be published as parties who exercise public authority. In a private trial, the case may still be of public interest. However, the level of interest is lower compared to a conflict involving a party with public authority. The public interest, in this case, is only related to the activity of the court instead of the identity of the litigants. Furthermore, the identity of the parties is only relevant if their conduct constitutes a violation of the rules established by public law, such as the rules related to financial transparency.[76] However, the regulation seems to create an overlap and ambiguity regarding the mode of conflict resolution if the court is faced with a conflict between the right to information and the protection of personal data.

Secondly, the regulation obliges the court to make public its general practice related to the reviewed cases, the decisions made, and the current cases for trial, by publishing the schedule of the upcoming cases. Thirdly, in criminal proceedings, according to Article 3.5, the court is obliged to publish general information about the defendant and the charge attributed to him. However, general information can create problems in practice regarding the possibility of the defendant being stigmatized after the end of the trial, especially in the case of guiltlessness.

The court is obligated to release certain information but must also be cautious about sharing details related to coercive measures in criminal proceedings. (Point 5.12 of the regulation) It's important to remember that the presumption of innocence remains until it is contrarily proven.[77] However, the regulation is unclear about whether information regarding the defendant should be made public, and if so, to what extent. The presumption of innocence is a constitutional right that can only be waived with conclusive evidence of guilt, beyond any reasonable doubt.[78] Personal information should be limited to what is relevant to the case at hand, and the court must ensure that media outlets do not publish the full names of suspects or individuals to whom criminal charges are attributed without a final verdict or in other cases from public statements from the individual in question.[79] Failure to do so could be considered an unjustified invasion of privacy and may result in legal action for compensation for unjust imprisonment and compensation for non-material damage as a result of unjustified publication of personal data.[80] This could also negatively affect the public confidence in the justice system and the financial cost for the state.

In addition, the financial data and asset declarations of administrative personnel, judges, and their families are publicly accessible to ensure transparency in the income of officials and senior public servants, as well as data related to court budgets and expenses. [81] However, financial data pertaining to private individuals are considered limited information, except in cases where financial transparency rules apply. Moreover, the court has a duty to inform the public about its activity on specific disputes under review or review, even without a request from the public. The court must make information about the resolution of current disputes available to the public on its website while ensuring the anonymization of the personal, sensitive, and judicial data that threaten the privacy of litigants or other parties involved.[82]

- COURT'S RESPONSIBILITY:

The court is a public authority responsible for delivering justice. As part of its duties, it must take measures to protect fundamental rights and freedoms, and ensure they are upheld. It can be challenging for the court to balance the need for transparency on one hand, and protection of privacy rights on the other hand. However, the court needs to perform its obligation to inform the public while also safeguarding individual rights. By doing so, the court can ensure that justice is delivered fairly and in compliance with legal requirements.

- THE IMPORTANCE OF PUBLIC HEARINGS:

The court hearings are generally public unless national interests, security, public order, morals, protection of minors, or the private life of parties are at stake, or if the interests of justice would be compromised. A public hearing cannot be held solely based on public interest without considering the test of proportionality when it comes to rights such as the right to privacy.

The court is obliged to provide the public with information about its activities and establish a transparency program to increase accountability and transparency. Nonetheless, the legitimacy of the court derives not only from the law but also from performing its obligation to be transparent and accountable to the public. Even in closed proceedings sessions, decisions must be made public.

The public has the right to access information that is produced or held by public authorities, which promotes integrity, transparency, and accountability. This is essential for strengthening democratic and institutional governance. It also helps people understand how the judicial system works and how justice is delivered. Consequently, the public can adopt a critical approach to compare the presumed constitutional situation with the reality. This can result in increased demands for accountability and transparency from judicial authorities.

- JUDICIAL DATA AND THE LAW ON DATA PROTECTION

The objective of the law on the protection of personal data is to guarantee fair and legal processing of personal data while ensuring the protection of fundamental human rights and the right to privacy.

Judicial data pertains to information about criminal, administrative, or civil decisions, as well as any documented data in civil, administrative, or criminal records. Sensitive data also includes information about criminal convictions. The concern is whether releasing this data could infringe on the individual's private life, freedom to choose their lifestyle after serving their sentence, and the risk of being stigmatized. Such stigmatization may harm their right to earn a living with dignity.

- CONSTITUTIONAL COURT ON DATA PROTECTION

The Constitution of the Republic of Albania provides individuals with the fundamental right to keep their personal data private unless the law permits its disclosure. Even without obtaining the subject's prior consent, data related to individuals may be processed and published in certain circumstances outlined by law. However, the law must have a specific purpose to justify such restrictions on privacy.

For instance, officials and public servants' data may be published, limiting their right to privacy due to their public function. The law must prioritize public interest over fundamental rights and freedoms. The court must follow the principles of legality, proportionality, and data collection purpose while exercising its constitutional functions.

When two rights conflict, the Constitutional Court states that the court must consider the intensity and degree of violation of private life, the necessity of intervention in a democratic society, the effectiveness and proportionality of the interference, and whether the litigant is exempt from the obligation to publish personal data. If the litigant is not exempt, the court must also consider whether publishing the identifying information serves justice.

- ECtHR ON DATA PROTECTION

Secondly, the ECtHR assessed the necessity of the dismissal regarding a democratic society. It was determined that any interference with the right to privacy must be justified by a purpose that aligns with the set goals in Article 8 and is necessary for a democratic society. The law in question aimed to combat corruption and restore public trust in the judiciary system. The ECtHR concluded that dismissal is a severe disciplinary action that should only be taken if there is consistent evidence regarding the individual's ethics, integrity, and professional ability.

- PROPORTIONALITY TEST

To sum up, the test of proportionality must be assessed in the context of fundamental rights and freedoms in conjunction and in accordance with public law. The personal data of the subject will be published only in cases where their publication does not threaten the rights and legitimate interests of the subject to which they belong. In any case of publication, the court is obliged to place the initials of the parties or to codify the parts that contain personal or sensitive data. However, even though at first sight, these rights may seem to protect two objects that are opposite to each other, this cannot be understood only in this way, but also as complementary, because although their object is different but not necessarily opposite. However, the limitation of fundamental rights and freedoms only by law serves as a guarantee for the holders of these rights, in order not to subject you to illegal actions of public authorities. The threshold of this restriction cannot in any case exceed the threshold established by the ECHR.

- PUBLIC'S RIGHT TO INFORMATION AND THE PUBLIC RELATIONS OFFICE

The Public Relations Office (PRO) is responsible for creating press statements that inform the public about specific cases or trial activities, even when not requested by the public. The PRO can advise the judge or the judicial panel on the advantages and disadvantages of taking a public stance. To do so, the PRO must have qualified personnel and experts in communication and public information, with relevant training in fundamental human rights and freedoms with a very narrow training on the right to information and privacy.

- ANONYMYZATION BY THE COURT

The court is obligated to inform the public through various means of communication and information, including its website, which should be updated regularly with information related to its activities. As the controller of

personal data in its activity, the court is authorized to process and control personal data within the framework of the exercise of its constitutional function, with limitations to protect basic human rights and freedoms, including the right to privacy. When publishing court decisions online, the court must consider anonymizing the identities of parties, third parties, witnesses, and experts by using initials or codes.

- DATA PROTECTION VS THE RIGHT TO INFORMATION

First, courts must provide unrestricted access to all court decisions at every level of trial. This is in accordance with the obligation that a court's decision must be public in any case, regardless of whether the court hearings were held private. However, there is a contrast noted within this regulation between the definitions of information with unlimited and limited access. Point 3.4 of the regulation provides information related to civil lawsuits, the parties involved, and the object of the lawsuit, under the category of information with unlimited access. Meanwhile, point 5.1 lists the personal data of each person under the category of information with limited access, contradicting point 3.4 on the generalities of the parties in a civil trial. Contrarily, in judicial-administrative hearings, the regulation foresees that the identity of the parties involved in the trial will be published as parties who exercise public authority. In a private trial, the case may still be of public interest. However, the level of interest is lower compared to a conflict involving a party with public authority. The public interest, in this case, is only related to the activity of the court instead of the identity of the litigants.

Furthermore, the identity of the parties is only relevant if their conduct constitutes a violation of the rules established by public law, such as the rules related to financial transparency. However, the regulation seems to create an overlap and ambiguity regarding the mode of conflict resolution if the court is faced with a conflict between the right to information and the protection of personal data.

Secondly, the regulation obliges the court to make public its general practice related to the reviewed cases, the decisions made, and the current cases for trial, by publishing the schedule of the upcoming cases. Thirdly, in criminal proceedings, according to Article 3.5, the court is obliged to publish general information about the defendant and the charge attributed to him. However, general information can create problems in practice regarding the possibility of the defendant being stigmatized after the end of the trial, especially in the case of guiltlessness.

- AMBIGUITY OF REGULATION no. 6777/5 “RULES FOR THE RELATIONSHIP BETWEEN COURT AND THE PUBLIC”

The court is obligated to release certain information but must also be cautious about sharing details related to coercive measures in criminal proceedings. (Point 5.12 of the regulation.) It's important to remember that the presumption of innocence remains until it is contrarily proven. However, the regulation is unclear about whether information regarding the defendant should be made public, and if so, to what extent. The presumption of innocence is a constitutional right that can only be waived

with conclusive evidence of guilt, beyond any reasonable doubt. Personal information should be limited to what is relevant to the case at hand, and the court must ensure that media outlets do not publish the full names of suspects or individuals to whom criminal charges are attributed without a final verdict or in other cases from public statements from the individual in question. Failure to do so could be considered an unjustified invasion of privacy and may result in legal action for compensation for unjust imprisonment and compensation for non-material damage as a result of unjustified publication of personal data. This could also negatively affect the public confidence in the justice system and the financial cost for the state.

In addition, the financial data and asset declarations of administrative personnel, judges, and their families are publicly accessible to ensure transparency in the income of officials and senior public servants, as well as data related to court budgets and expenses.

[1]Toffler Alvin, The Third Wave (Collins 1980)

[2]Webster Frank, Theories of the information society, 3d Ed. United Kingdom (Routledge 2006). Available from: http://www.kultx.cz/wp-content/uploads/theories-of-the-information-society-by-frank-webster.pdf

[3]Flanagan Anne, EU Freedom of Information: Determining where the Interest Lies, 13, European Public Law, Issue 4, pp. 595-932, (2007), Available from: https://kluwerlawonline.com/journalarticle/European+Public+Law/13.4/EURO2007035

[4] Lynskey Orla, Deconstructing Data Protection: the 'Added-Value' of a Right to Data Protection in the EU Legal Order the International and Comparative Law Quarterly, Vol. 63, No. 3, pp. 569-597 (2014)

[5] McDonagh, M., The Right to Information in International Human Rights Law', Human Rights Law Review, 13(1), pp. 25-55 (2013) Available from: doi:10.1093/hrlr/ngs045

[6] Council of Europe, 'Tromsø Convention" <https://www.coe.int/en/web/access-to-official-documents> Accessed 10 August 2023

[7] General Data Protection Regulation (2016), Article 2 (1): "This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system." Available from: https://eurlex.europa.eu/eli/reg/2016/679/oj

[8] Ibid, Article 2 (2): "This Regulation does not apply to the processing of personal data: (a) in the course of an activity which falls outside the scope of Union law; (b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU; (c) by a natural person in the course of a purely personal or household activity; (d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security."

[9] Banisar David, The Right to Information and Privacy: Balancing Rights and Managing Conflicts, World Bank Institute (2011). Available from: https://www.iprs.si/fileadmin/user_upload/Pdf/Publikacije_ostalih_pooblascencev/Right_to_Information_and_Privacy__banisar.pdf

[10] Ibid

[11] Supra note 5

[12] Supra note 7, Article 3 (1) lays down its territorial scope: "This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not."

[13] Case C-131/12, Google Spain v APED, judgment of May 13, 2014, ECLI:EU:C:2014:317.

[14] Krishnamurthy V, "A Tale of Two Privacy Laws: The GDPR and the International Right to Privacy" (2020) 114 AJIL Unbound 26. Available from: https://www.cambridge.org/core/journals/american-journal-of-internationallaw/article/tale-of-two-privacy-laws-the-gdpr-and-the-international-right-toprivacy/8F51BC461CEC2B557962643B6E24D390

[15] Diker Vanberg, Aysem. "Informational privacy post GDPR – end of the road or the start of a long journey? The International Journal of Human Rights", 25(1), pp. 52-78. ISSN 1364-2987 (2021). Available from: https://research.gold.ac.uk/id/eprint/31301/1/28835%20DIKER%20VANBERG_Informational_Privacy_Post_GDP R_%28AAM%29_2020.pdf

[16] Electronic Privacy Information Center, Article 29 Working Party, <https://epic.org/article-29-workingparty/#:~:text=The%20Working%20Party%20on%20the,Member%20States%2C%20the%20European%20Data> Accessed 10 August 2023.

[17] Brasher, E. "Addressing the Failure of Anonymization: Guidance from the European Union's General Data Protection Regulation." Columbia Business Law Review, 2018(1), 209–253. Available at: https://doi.org/10.7916/cblr.v2018i1.1217

[18] Supra note 14

[19] Supra note 7, Article 4 (1): "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); 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."

[20] Ibid

[21] Supra note 7

[22] Spiekermann-Hoff, S. "The Challenges of Privacy by Design. Communications of the ACM (CACM)", 55(7), 34 – 37 (2012). Available from: https://doi.org/10.1145/2209249.2209263

[23] Supra note 7, Article 5.1.(c): "Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')"

[24] Ibid, Article 4 (5): 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

[25] Oksanen , A , Tamper , M , Tuominen , J , Hietanen , A & Hyvönen , E 2019 , ANOPPI: A Pseudonymization Service for Finnish Court Documents . in M Araszkiewicz & V Rodríguez-Doncel (eds) , Legal Knowledge and Information Systems . Frontiers in Artificial Intelligence and Applications , IOS PRESS , pp. 251- 254 . https://doi.org/10.3233/FAIA190335

[26] Čtvrtník, Mikuláš. Archives and Records: Privacy, Personality Rights, and Access (2023). Available from: https://www.researchgate.net/publication/366898441_Archives_and_Records_Privacy_Personality_Rights_and_Access

[27] Noora Arajärvi, Livia Holden (Dir.). "GDPR compliant guidelines for processing personal data in legal documents" (2021). Available from: https://hal.science/hal-03527460/document

[28] Court of Justice of the European Union PRESS RELEASE No 96/18 Luxembourg, 29 June 2018

[29] Court of Justice of the European Union, Directorate-General for Library, Research and Documentation, Anonymity of the parties on the publication of court decisions. (2017) <https://curia.europa.eu/jcms/upload/docs/application/pdf/2021-02/ndr_2017-002_neutralisee-en.pdf>. Accessed July 25 2023.

[30]Ibid

[31] Ibid

[32] Ibid

[33] Ibid

[34] Supra note 28

[35] Ibid

[36] Maxeiner, James R. "Freedom of Information and the EU Data Protection Directive," Federal Communications Law Journal: Vol. 48: Iss. 1, Article 4. (1995) Available at: https://www.repository.law.indiana.edu/fclj/vol48/iss1/4

[37] Decision no. 16 date 11.11.2004 of Constitutional Court of Republic of Albania

[38] Article 2/1 of Law no. 119/2014 "On the Right to Information"

[39[Article 42 of the Constitution of the Republic of Albania

[40] Supra note 2., art. 3/1.

[41] Supra note 3., art. 15.

[42] Article 6 of the European Convention of Human Rights

[43] Ibid.

[44]Supra note 2., art. 4 & 6.

[45] Article 6 of ECHR; Articles 42 & 146/2 of Constitution of the Republic of Albania; Article 26 of "The Code of Civil Procedure of the Republic of Albania" amended by law. 44/2021, dated 23.03.2021.

[46] Ibid.,

[47] Supra note 2., art. 1/3 & 2/1(a).

[48] Supra note 1.

[49] Supra note 3., art. 17/2.

[50] Article 1 & 2 of Law no. 9887 dated 10.03.2008 "On Protection of Personal Data" amended by Law no. 120/2014

[51] Ibid., Article 3/1.

[52] Ibid., art. 3/2 & 3/4.

[53] Case XHOXHAJ v. ALBANIA dated 09/02/2021, European Court of Human Rights.

[54] Supra note 2., art. 17/2.

[55] Article 1., Chapter IV "On Publication of Personal Data" of Instruction no.15 date 23.11.2011 "On Processing and Publication of Personal Data in Judicial Sector."

[56] Supra note 14., art. 10.

[57] Supra note 1.

[58] Ibid.

[59] Ibid.

[60] Ibid.

[61] Supra note 17.

[62] https://www.idp.al, "Handbook of European Data Protection Law" accessed on 30 July 2023.

[63] Supra note 19., art.1.

[64] Ibid., art.2.

[65] Article 1/1(a)(b)(c) of Regulation no. 6777/5 "Rules for the Relationship between Court and the Public."

[66] Ibid., art. 1/1(c)(ç).

[67] Supra note 29., art. 3/1.2(ç).

[68] Supra note 19., art. 1, Chapter II.

[69] Ibid., art. 4., Chapter IV.

[70] Ibid

[71] Supra note 29., art. 1/2(ç).

[72] Ibid.

[73] Ibid.

[74] Ibid., art.3, section VI "Information of the Public on Court's Documents"

[75] Supra note 9.

[76] Supra note 29, art.5.4 Section 5 "The List of Documents with Limited Access."

[77] Supra note 3., art. 30.

[78] Article 4 of Law no. 7905, date 21.3.1995 "Criminal Procedure Code of the Republic of Albania" amended by law.35/2017.

[79] Supra note 26.

[80] Supra note 42., art. 268.

[81] Supra note 29.

[82] Ibid.