AMONG THE WEAKNESSES OF CONSTITUTIONAL LAW

Mircea Criste
Professor at the West University of Timisoara

Elpis has a tradition of launching debates on highly interesting and complex topics. Such is the theme proposed for this issue of the journal, *Weakness and Effectiveness in Law*.

Law, as a social and political phenomenon, is meant to ensure order in society and to contribute – through appropriate regulations – to its evolution in all areas. From this perspective, to avoid descending into chaos, the law must be robust and capable of providing the best solutions to society's challenges.

However, the bad news is that the law is not perfect – it has its weaknesses. The law must track developments in society and respond with regulations that keep pace and direction with those changes. Yet this process is far from simple: in its course, the law's response can be delayed or only approximate, thereby bringing its weaknesses to the forefront.

On the other hand, the good news is that the law possesses – and indeed utilizes – mechanisms of self-regulation to adapt to social and economic changes. Through suitable legislation, judicial interpretation, and recourse to fundamental legal principles, the legal system manages to maintain balance in the community.

Law exhibits weaknesses across all its branches – from international law to procedural law – a point frequently noted in various studies. There are weaknesses in the regulation of certain powers, which are often insufficient or uncoordinated. There are also weaknesses in the judicial system stemming from defective methods of appointing judges (such as lack of transparency, political interference, and compromised judicial independence) or from inadequate training of judges. These weaknesses can have an even greater impact when combined with the absence or ineffectiveness of judicial oversight (particularly in international law).

Another weakness of the legal system is inadequate regulation – whether under-regulation or, conversely, over-regulation – as both can impede the uniform interpretation and application of the law. This weakness can be further exacerbated by the *tale quale* importation of external legal models and regulations that are sometimes alien to the society's own legal culture.

These are only a few examples, but they suffice to support the conclusion that, in the face of such weaknesses, the law ceases to keep pace with the evolution of social relations. Instead, it acts more as a brake on society than as a driving force.

Constitutional law is no exception to this picture. In fact, its weaknesses have the most significant societal impact, because constitutional law not only establishes and regulates the relationships between public institutions in a democracy, but also promotes and safeguards citizens' rights. Therefore, whenever priorities are asserted in arranging fundamental rights – when protecting one right requires accepting additional limitations on the exercise of another – we are confronted with the weaknesses of constitutional law.

To support this claim, I will examine instances of fundamental rights coming into conflict, with special attention to the right to private, intimate and family life. The exercise of this right is undermined, on one hand, by interference from the right to freedom of expression, and on the other, by threats emerging from the online environment and virtual platforms.

1. Private Life vs. Freedom of Expression

The doctrinal and jurisprudential issues that arise concerning fundamental rights revolve around the exercise of those rights – especially the scope of their exercise. For this reason, avoiding conflicts between rights will always remain a serious challenge for any framer of a constitution.

The right to intimate, family, and private life implies that everyone should enjoy the confidentiality of their private life, have their right to their own image respected, and not have personal data made public without their explicit consent. These requirements have become increasingly difficult to uphold amid the unprecedented expansion of mass media. The media, invoking necessity and everyone's right to information, often push beyond the permissible boundaries of privacy, resulting in a collision between the right to private life and one's personal image, on the one side, and freedom of expression and the public's right to information, on the other. Not infrequently we hear – particularly from public figures – accusations that acts of libel or defamation have been perpetrated through the media. Likewise, journalists often complain of harassment and constraints on press freedom through lawsuits brought against them.

Looking across time, if we imagine the edifice of fundamental rights, freedom of expression lies at its foundation. It belongs to the first generation of fundamental rights and freedoms championed by the French Revolution, which – in the Declaration of the Rights of Man and of the Citizen – proclaimed the freedom to communicate thoughts and opinions as one of the most valuable human rights.

Human freedom can be understood in two dimensions: one physical, the other pertaining to conscience. Thus, the French revolutionaries, in the first articles of their rights charter, proclaimed the physical liberty of the individual, followed immediately by the affirmation of freedom of conscience and freedom of expression. No one may be accused, arrested, or detained except under circumstances defined by law (Articles 7–8), and likewise, no one may be prosecuted or harassed for their opinions, and the expression of those opinions cannot be curtailed unless it is abusive (Articles 10–11).

However, the exercise of the right to free expression is not absolute. A first limitation is, of course, the obligation not to cause harm to others – allowing each person to enjoy their own rights (Article 4 of the Declaration of the Rights of Man and of the Citizen). A significant and essential limitation on freedom of expression is that it must not prejudice a person's dignity, honor, private life, or their right to their own image. Especially in the period after the Second World War, human dignity has emerged as a decisive principle in many situations, tipping the balance when different interests collide by giving precedence to the interest that upholds human dignity.

When it comes to freedom of expression via the mass media, it must be noted that this freedom comes with obligations and responsibilities. The guarantees provided to journalists

under Article 10 of the European Convention on Human Rights are contingent on journalists acting in good faith, providing accurate and credible information while respecting journalistic ethics.

When judges must determine to what extent the public's right to information takes priority, they need to consider whether an image published in the media is justified by a legitimate public interest in its content. In practice, the inquiry is essentially limited to asking whether the publication of that image contributes to the formation of public opinion. Thus, one can say that publishing a photograph is justified only if, without its publication, the public would have been deprived of the opportunity to form an informed opinion. Conversely, freely photographing public figures for media publication – when those figures are not in a private space – is not something constitutionally guaranteed[1].

At times, under the banner of necessity and the public's right to know, the permissible limits of privacy are breached. Public figures, especially, complain of slanderous allegations leveled against them in the media, just as journalists complain of harassment and the curtailment of press freedom through lawsuits filed against them. These reactions seem to suggest a collision of two sets of rights: on the one hand, the right to private life and to one's own image; on the other, freedom of expression and the right to information. This clash is exemplified by the debate over criminalizing defamation – treating insult and libel as criminal offenses is perceived as a restriction on free expression, implemented to defend values that lie at the heart of a democratic society.

Legal doctrine speaks of a "conflict of rights" when the obligations necessary to fully realize two or more rights cannot be satisfied simultaneously because the fulfillment of one would nullify the other. Such a situation may occur when what one right demands is forbidden by another right, or when two rights impose different obligations that cannot be met at the same time.

In Romania, both constitutional and ordinary courts have grappled with the issue of decriminalizing defamation. The Constitutional Court, when reviewing the constitutionality of the law that decriminalized insult and calumny (libel), held that there is no incompatibility between the principle of freedom of expression and the criminalization of insult and defamation that would necessitate decriminalizing these offenses. Romania's High Court of Cassation and Justice, by contrast, took the view that the Criminal Code provisions on insult and calumny were no longer in force, reasoning that repealing a repealing act cannot serve to reinstate the original act. However, the supreme court in this instance conflated *repeal* with *unconstitutionality*, since a finding that a provision is unconstitutional is not equivalent to repealing it. Repeal – a power vested solely in the issuing legislative authority or a superior authority – applies to a provision that was valid throughout its existence (otherwise we would speak of nullity or non-existence of the act). Unconstitutionality, by contrast, removes the effect of a provision that was flawed from the moment of its issuance; if the provision deemed unconstitutional is one that repealed a law, then it is the repealing effect itself that must be removed.

---

[1] Decision of the First Senate of the Constitutional Court of the Federal Republic of Germany of February 26, 2008, http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080226_1bvr160207.html.

It is difficult to see how one respects a Constitutional Court decision declaring a repealing provision unconstitutional if one continues to give effect to that very provision. Yet that is exactly what the High Court did when it concluded that the criminalization of insult and defamation had been expressly repealed on the basis of the very legal article the Constitutional Court had invalidated.

Returning to the supposed collision between these fundamental rights – private life and personal image *versus* freedom of expression and the right to information – we can conclude that this is not truly a clash of rights at all, but rather an abusive exercise of rights. It is an abuse of *the right to one's image* when, under its shelter, someone attempts to cover up and silence various illegalities. And it is an abuse of *freedom of expression* when it is employed either to knowingly circulate falsehoods about a person or to violate that sphere of intimacy which every individual is entitled to enjoy.

2. Private Life vs. Personal Security

The restriction of personal rights in the name of collective rights or public interests – such as national security, public order, or crime prevention – has always been a sensitive matter of regulation. It necessitates maintaining a just balance between individual rights and interests on the one hand, and the interests of society on the other[2].

The question of how constitutional law can safeguard the right to private life took on new urgency after the terrorist attack of September 11, 2001 in New York. In its wake, a series of measures were adopted worldwide to prevent similar events. All of these measures dealt primarily with monitoring citizens' daily activities and storing information about them.

Romanian legislation on the retention of data generated or processed by public electronic communications network providers and electronic communications service providers transposes Directive 24 of March 15, 2006, of the European Parliament and of the Council, adopted following the terrorist attacks of July 7, 2005, in London[3]. The main objective of this Directive was to harmonise the legislation of Member States on the obligations of providers of publicly available electronic communications services or public communications networks to retain certain data generated or processed, in order to ensure the availability of such data for the prevention, investigation, detection and prosecution of serious crimes, such as organised crime and terrorism.

Directive 24 came under scrutiny by the judges in Luxembourg after two preliminary questions were referred to them in 2012 by the High Court of Ireland and the Constitutional Court of Austria.

The request from the Irish High Court (Case C-293/12) concerned the action brought by Digital Rights Ireland Ltd. against the Minister for Communications, Marine and Natural Resources, the Minister for Justice, Equality and Law Reform, the Commissioner of the Garda

---

[2] Romania's Constitutional Court Decision (CCD) No. 1258/2009, published in the *Official Gazette* No. 798/2009.

[3] On July 13, 2005, the Council reaffirmed in its statement condemning the terrorist attacks in London the need to adopt, as soon as possible, common measures on the retention of telecommunications data. Directive 24 of 2006 requires providers of publicly available electronic communications services or public communications networks to retain certain data generated or processed by those providers.

Síochána, Ireland, and the Attorney General, challenging the legality of national legislative and administrative measures relating to the retention of electronic communications data.

The request sent by the Constitutional Court in Vienna (Case C-594/12) concerned constitutional proceedings brought by the government of the province of Carinthia and a number of other applicants, concerning the compatibility of the Austrian law transposing Directive 24 of 2006 with the Federal Constitution.

In its judgment of 8 April 2014, the Court of Justice of the European Union (CJEU) ruled that Directive 2006/24 violated the provisions of Articles 7, 8, and 52(1) of the Charter of Fundamental Rights of the European Union[4].

The Court of Justice based its reasoning on the relationship between the contested directive and the provisions of the Charter of Fundamental Rights of the European Union, finding that the retention of the data in question was compatible with the Charter. However, the measures provided for in the Directive constitute an interference with the rights guaranteed by Articles 7 and 8 of the Charter, in breach of the principle of *proportionality* between the measures taken and the public interest protected.

The Court noted in this regard that the data covered by the Directive lead to very precise conclusions about the private lives of the persons whose data have been stored, which may concern their daily habits, their permanent or temporary places of residence, their daily or other movements, their activities, the social relationships of those persons and the social circles they frequent, and that, in those circumstances, even if the storage of the content of communications and information consulted using an electronic communications network is prohibited, the storage of such data may affect the use by subscribers or registered users of the means of communication provided for in that directive and, consequently, their freedom of expression, guaranteed by Article 11 of the Charter.

It has also been found that the retention of data for the purpose of ensuring that the competent national authorities have access to it directly and specifically concerns private life and, consequently, the rights guaranteed by Article 7 of the Charter. Such data storage also infringes Article 8 of the Charter, as it constitutes the processing of personal data and must comply with the data protection requirements arising from that article. Consequently, the Court of Justice concluded that the obligation imposed by Directive 24 on electronic communications service providers to retain data relating to a person's private life and communications for a certain period of time constitutes both an interference with the rights guaranteed by Article 7 of the Charter and an interference with the fundamental right to the protection of personal data guaranteed by Article 8 of the Charter, in so far as it provides for the processing of personal data. These interferences are extensive and must be regarded as particularly serious, all the more so since the fact that the data are retained and subsequently used without the subscriber or registered user being informed of this is likely to give rise to a feeling among the persons concerned that their private lives are under constant surveillance.

The Court in Luxembourg also looked at whether the principle of proportionality had been respected, concluding that the general interest objective of the Directive, even if

[4] Decision of April 8, 2014,https://www.scribd.com/doc/216980523/Judgment-of-the-ECJ-in-Digital-Rights-Ireland-data-retention-challenge

fundamental, cannot justify the need for measures such as those provided for in the same European law for the purpose of combating the crimes indicated therein.

In order to give effect to the provisions of Articles 7 and 8(1) of the Charter, the European Directive should have included clear and precise rules on the content and application of the data retention measure and provided for a number of limitations, so that persons whose data have been retained benefit from sufficient safeguards to ensure effective protection against abuse and any unlawful access or use.

It was also noted in the judgment of 8 April 2014 that Directive 24/2006 concerned all persons using electronic communications services, without them being, even indirectly, in a situation likely to trigger the initiation of criminal proceedings. It was also emphasized that the Directive did not provide for any exception for persons whose communications are subject to professional secrecy under national law.

Another violation of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union was identified in the fact that Directive No. 24/2006 does not provide for any objective criteria allowing the delimitation of access by the competent national authorities to data and their subsequent use for the purpose of prevention, detection, or prosecution of crimes that can be considered serious enough to justify such interference. Moreover, it was found that the directive did not expressly provide that access by the competent national authorities to stored data and their subsequent use must be strictly limited to the prevention and detection of precisely defined crimes or the prosecution of such crimes.

The same judgment also held that Directive 24 does not lay down objective criteria limiting to what is strictly necessary the number of persons who have access to and can subsequently use the stored data. There was no provision for prior review by an independent court or administrative body to limit the access of national authorities to the stored data and their use to what is strictly necessary for the achievement of the objective pursued, nor was there any provision for Member States to establish such limitations.

With regard to the duration of data storage, it was noted that the Directive required data to be stored for a period of 6 to 24 months, without providing for objective criteria to limit data storage to what was strictly necessary and without distinguishing between categories of data according to their usefulness for achieving the objective pursued or according to the persons concerned.

Finally, it was found that the Directive did not require the stored data to be kept within the European Union, so that the control of compliance with the protection and security requirements laid down in Article 8(3) of the Charter, which is an essential element of the protection of individuals with regard to the processing of personal data, was not fully guaranteed.

Romania's Constitutional Court had actually confronted the data retention issue earlier, in Decision No. 1258 of October 8, 2009, which reviewed the constitutionality of Law No. 298/2008 (the domestic "data retention" law). The challenged provisions of that law required providers of public electronic communications services to retain the traffic and location data of individuals and legal entities, along with associated data needed to identify the user, and to make those data available to competent authorities for use in the investigation, detection, and prosecution of serious offenses. The Constitutional Court observed that the law's provisions

failed to clearly and unambiguously define the term *related data*. This lack of a precise legal definition to delineate exactly which data were necessary for identifying users opened the door to potential abuses in the retention, processing, and use of data stored by the service providers. Furthermore, the Court emphasized that any restriction of the exercise of the right to private life and the secrecy of correspondence (as well as freedom of expression) must be implemented in a clear, foreseeable, and unequivocal manner, in order to eliminate as far as possible the risk of arbitrariness or abuse by authorities.

The Court found similarly ambiguous wording in a provision that allowed state bodies responsible for preventing and countering threats to national security to access data retained by communications service providers. Since the law did not define *unequivocally* what constituted *threats to national security*, it would be possible for various ordinary actions, information, or routine activities of individuals or entities to be arbitrarily deemed as such threats. Moreover, individuals could be classified as suspects without their knowledge and without any chance to prevent the consequences of the law's application through their own conduct. In this way, a person who is merely the recipient of a telephone call could be subjected to data retention about their private life without any action or choice on their part – solely due to the caller's behavior, which the recipient cannot control. Although the recipient is a passive party in the communication, they could unwittingly become a suspect under the stringent conditions in which state authorities carry out criminal investigations. In the Constitutional Court's view, such an arrangement made the intrusion into an individual's private life excessive.

In matters of personal rights – such as the right to private life and freedom of expression – and in the realm of personal data processing, the universally recognized principle is to guarantee and uphold these rights, i.e. to preserve confidentiality. Accordingly, the state's obligations are predominantly negative in nature: the state must refrain from interfering, as far as possible, in the exercise of these rights and freedoms. This principle was violated by Law No. 298/2008, which established continuous retention of personal data as a rule, for a period of six months from the time of their interception. Invoking the case law of the European Court of Human Rights (ECtHR)[5], the Constitutional Court underscored that a legal obligation requiring the continuous retention of personal data cannot turn an exception to the effective protection of the right to private life and free expression into an absolute rule. In other words, the law had inverted the norm: it transformed what should have been an exception into a blanket policy, regulating the right in a predominantly negative manner and diminishing the primacy of the right's protective aspect.

Decision No. 1258/2009 also assessed compliance with another essential condition for restricting fundamental rights: the principle of proportionality, which requires that any restrictive measure correspond to the situation that prompted it, and that it cease once the underlying cause has disappeared. Law 298/2008, however, imposed an obligation of continuous data retention without accounting for the need to terminate the measure once its precipitating cause had been resolved. The interference with the free exercise of the right occurred incessantly and without any concrete triggering event – solely for the purpose of crime prevention or the discovery of serious offenses.

[5] Judgment of July 12, 2001, delivered in the case of Prince Hans-Adam II of Liechtenstein v. Germany.

Even absent any requirement to retain the content of communications, the Court held that retaining all of the other data (identifying the caller and recipient, the source, destination, date, time and duration of the communication, the type of communication, the devices used, the location of mobile equipment, and *other related data*) still constituted a violation of freedom of expression.

Moreover, even if the restriction of the exercise of certain fundamental rights may be justified in consideration of collective rights and public interests relating to national security, public order, or crime prevention, the adoption of surveillance measures, without adequate safeguards can lead to the destruction of democracy under the pretext of defending it[6].

Following Decision 1258/2009, Law No. 82/2012 was adopted, which in turn was challenged before the Constitutional Court[7]. The Court found in Decision No. 440/2014 that the possibility for state bodies with responsibilities in the field of preventing and countering threats to national security to have access to data retained by providers of public electronic communications services and networks is also found in Law No. 82/2012, maintaining a situation similar to that provided for in the old law that was declared unconstitutional.

Law 82/2012 maintained the continuous data retention obligation, which itself was deemed a ground of unconstitutionality. The interference with fundamental rights – private and family life, the secrecy of correspondence, and freedom of expression – was of great magnitude and had to be considered particularly severe. Moreover, the fact that data were being kept and later used without the subscriber or registered user being informed was likely to instill in individuals the feeling that their private lives were under constant surveillance. The processing of data under Law 82/2012 could yield highly detailed insights into the private lives of persons whose data were retained – revealing their everyday habits, places of permanent or temporary residence, daily travels or other movements, activities undertaken, social relationships, and the social circles they frequent. Such an intrusion into the exercise of the right to private life and the secrecy of correspondence (and into freedom of expression) must therefore occur in a clear, foreseeable, and unambiguous manner so as to eliminate, as far as possible, the potential for arbitrariness or abuse by the authorities.

The Court also noted an absence of objective criteria to limit the number of officials who could access and use the retained data. Access by national authorities to the stored data was not, in all cases, conditioned on prior review by a court or an independent administrative body that would restrict access and use to what was strictly necessary to achieve the intended objective.

Finally, in reviewing the constitutionality of this *Big Brother* legislation, Decision 440/2014 considered legal developments and jurisprudence in other EU states. It cited a March 2, 2010 judgment of the German Constitutional Court, which underscored the importance of retaining telecommunications traffic data for preventive purposes but also stressed the need for sufficiently strict and clear rules regarding data security and the limitation of data use, in order to ensure transparency and legal protection. The Karlsruhe court cautioned that such data

[6] ECtHR judgment of 6 September 1978, Klass and Others v. Germany, paragraph 49, https://hudoc.echr.coe.int/eng#{"itemid":["001-57510"]}
[7] CCD No. 440/2014, published in the *Official Gazette* No. 653/2014.

retention constitutes a far-reaching intrusion – even when the content of communications is not stored – because the retained metadata enable a detailed understanding of an individual's intimate sphere, particularly with respect to their social or political affiliations, preferences, inclinations, and weaknesses. This allows for the creation of revealing personal profiles and creates the risk of citizens being subjected to investigation without cause. In the specific case, the German court found a violation of the principle of proportionality: the provisions in question referenced only a general "necessary diligence" in telecommunications, but they diluted concrete security requirements by leaving them largely to the discretion of telecom operators. The law imposed no sufficiently high security standards on those operators, and notably, it set heavier penalties for failing to retain data than for failing to secure the data.

The Romanian Constitutional Court also pointed to a March 22, 2011 decision of the Czech Constitutional Court, which struck down legal provisions for not offering citizens sufficient guarantees against the abusive use of stored data, and a December 11, 2008 ruling of the Bulgarian Supreme Administrative Court, which annulled a provision that had allowed the Interior Ministry to retain data on computer terminals without judicial authorization.

3. Private Life vs. the Online and Virtual Environment

Turning to a different aspect of the online world, a widely publicized incident highlighted the clash between privacy and security in the digital realm. On December 2, 2015, seemingly without warning, two employees of a disability services center in San Bernardino carried out an attack, killing 14 people and wounding 22 others at a staff gathering. Before they were killed in a shootout with police, the attackers tried to destroy the phone and computer they had used. In the aftermath, the FBI recovered an iPhone 5c belonging to one of the terrorists but, after multiple attempts, announced on February 9, 2016, that it could not unlock the device due to the iPhone's strong encryption and security features. The Bureau asked Apple to create a new version of the iOS operating system to install on the phone—one that would bypass or disable its security measures.

Apple, invoking its policy of not compromising the security of its products, refused to create such a backdoor. The FBI then obtained a court order from a federal judge compelling Apple to assist in unlocking the phone. The order was based on an eighteenth-century statute – the *All Writs Act* of 1789 – which authorizes U.S. federal courts to issue any orders necessary and appropriate to aid their investigations, consistent with the customs and principles of law[8]. Apple challenged the applicability of that law to this case. The legal standoff ended when the FBI ultimately withdrew its request, stating that it had found an alternative method to access the phone's data.

We must also consider the new modalities of exercising freedom of expression and communication in the online environment and on virtual platforms. This new reality has led to the articulation of a new right for citizens: the *right to be forgotten*, or right to erasure, as part of the broader framework of personal data protection. Individuals have the right, under certain conditions, to request search engines to remove links to personal information about them when those informations are inaccurate, inadequate, irrelevant, or excessive in relation to the

[8] The invocation of this law has led to other famous cases that have shaped the history of North American justice, such as the well-known *Marbury v. Madison.*

purposes of data processing[9]. The right to be forgotten is not absolute; it must be balanced against other fundamental rights like freedom of expression. For this reason, decisions on delisting are made case by case, considering factors such as the type of information, its sensitivity with respect to private life, and the public's interest in accessing that information. The role a person plays in public life can also be an important factor. It is evident, however, that this remedy has limited effectiveness, as some publications have simply re-posted information that was delisted, thereby reintroducing it into the online sphere.

On a related note, the events involving Facebook in 2018 – namely the *Cambridge Analytica* scandal and the manipulation of citizens via social media, which resurfaced dramatically during Romania's December 2024 presidential elections – will change how the right to privacy is viewed and protected going forward. It stands as a lesson that no future constitution-framer will be able to ignore.

In summary, the question that arises is: Should general communal security be given precedence whenever there is even a mere suspicion of a threat, at the cost of relinquishing essential elements of personal freedom that have been secured through centuries of effort and sacrifice? Or must personal freedom be preserved as the supreme value, even at the risk of any sacrifice? To put it even more simply: is individual freedom a greater value than personal safety and collective security?

As the *Apple* case illustrates, this dilemma tends to split people into two polarized camps. Good-faith defenders of liberty end up being portrayed as accomplices of the terrorists who threaten the free and democratic world. Conversely, those who absolutize societal security are suspected of seeking – whether consciously or not – to regiment society and to transform individual freedom from a natural right into a privilege granted by those who control society.

Since both freedom and individual safety are attributes of each of us, it becomes increasingly clear that we are in the position of Buridan's donkey – forced to choose between two things that are equally necessary and inalienable, with the prospect of ultimately losing both.

[9] CJEU, Grand Chamber, Judgment of May 13, 2014, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131