DE CIFRIS KOINE
Book Series
Volume III

ERUDITORUM ACTA 2024

DE CIFRIS KOINE
Series Editorial Board

DE CIFRIS KOINE
Book Series

De Cifris Koine è una collana editoriale curata da De Cifris Press, marchio dell'associazione nazionale De Componendis Cifris dedicata allo studio e alla divulgazione della crittografia e delle discipline correlate.

Questa collana rappresenta un punto di riferimento per la comunità crittografica italiana, offrendo una panoramica delle ricerche e delle innovazioni nel campo. Attraverso la pubblicazione degli atti di conferenze e workshop, De Cifris Koine fornisce non solo approfondimenti scientifici, ma anche contributi divulgativi, mettendo in luce i progressi e le attività dei principali esponenti in questo ambito.

La serie abbraccia un ampio spettro di argomenti, estendendosi oltre la crittografia stessa per includere le sue molteplici applicazioni e intersezioni con altre discipline. Tra queste, si annoverano la teoria dei codici, vari rami della matematica come l'algebra, la teoria dei numeri e la geometria, l'informatica con un focus particolare sulla cybersecurity e sull'informatica teorica, nonché l'ingegneria elettrica, le telecomunicazioni, la storia e gli aspetti legali legati alla crittografia.

Gli articoli pubblicati in questa collana sono accettati in tre lingue: italiano, inglese e francese.

La periodicità della pubblicazione è trimestrale.

De Cifris Koine is a book series published by De Cifris Press, publishing house of the national association De Componendis Cifris, whose activities focus on cryptography and related topics. De Cifris Koine volumes form the voice of the Italian cryptographic community, as they collect communications from both scientific and educational events and summaries of papers of its members and of their activities. In particular, De Cifris Koine hosts conference and workshop proceedings, including short abstracts.

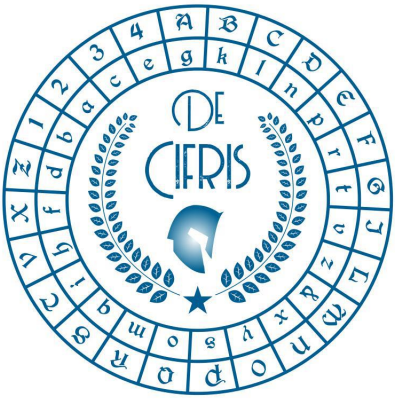
Topics covered in De Cifris Koine volumes relate to cryptography and its applications to and connections with other disciplines, as for example coding theory, maths (mainly algebra, number theory and geometry), computer science (mainly cyber security and theoretical computer science), electronic engineering, telecommunication engineering, history of cryptography and law.
Accepted articles are either in Italian, English or French.
Volumes are published quarterly.

La De Cifris Koine est une collection publiée par la De Cifris Press de l'association nationale italienne De Componendis Cifris. Elle est consacrée à l'étude et à la diffusion de la cryptographie et des disciplines connexes.

Cette collection est une référence importante pour la communauté cryptographique italienne, offrant une vue d'ensemble de la recherche et des innovations dans ce domaine. Grâce à la publication d'actes de conférences et de groupes de travail (workshops), la De Cifris Koine fournit non seulement des contributions scientifiques académiques, mais aussi des contributions à destination du grand public, mettant en lumière les progrès et les activités des principaux acteurs et des principales actrices du domaine.

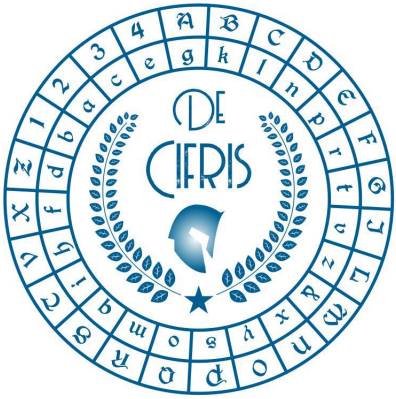
Les articles de cette collection couvrent un large éventail de sujets allant de la cryptographie à ses nombreuses applications et intersections avec d'autres disciplines. On y retrouve notamment la théorie des codes, diverses branches des mathématiques telles que l'algèbre, la théorie des nombres et la géométrie, l'informatique, avec un accent sur la sécurité informatique et l'informatique théorique, ainsi que le génie électrique, les télécommunications et les aspects juridiques de la cryptographie. Les articles soumis à la De Cifris Koine sont acceptés en italien, anglais et français. La fréquence de publication est trimestrielle.

ERUDITORUM ACTA 2024



Edited by:

– *Antonino Alì*,
Università di Trento, Italy.
– *Massimiliano Sala*,
Università di Trento, Italy.



Pubblicazione trimestrale di proprietà dell'associazione nazionale di crittografia
De Componendis Cifris

Autorizzazione del Tribunale di Milano in data 23 - 02 - 2024
Num. R.G. 1315/2024 Num. Reg. Stampa 22
ISSN 3034-9796 - ISBN 979-12-81863-02-6

Editore: De Componendis Cifris APS.
Marchio Editoriale: De Cifris Press.
Direttore responsabile: Massimiliano Sala
Redazione: Antonino Alì, Nadir Murru
Luogo di pubblicazione: Via Gianfranco Zuretti 34 - 20125 Milano
e-mail: editorial@decifris.it
Stampa in proprio
Numero 3 - Pubblicato il 01 - 09 - 2024

PREFACE

Questo volume, raccogliendo i contributi presentati durante il nostro convegno *"De Cifris Eruditorum 2024"*, offre un'analisi multidisciplinare della crittografia, tracciando il suo percorso storico ed esplorando, da un punto di vista giuridico, le sue attuali applicazioni e implicazioni.
I tre interventi storici toccano sia l'età classica, sia il Medio Evo, sia il Rinascimento. I due contributi giuridici si concentrano sulla cyber security e sul delicato equilibrio tra il rispetto dei diritti fondamentali e la necessità di sicurezza.

This volume contains all talks given at our conference *"De Cifris Eruditorum 2024"*. It offers a multidisciplinary approach to cryptography, starting from its historical evolution and arriving at exploring its current applications from a legal point of view.
The three historical talks touch on the cryptographic evolution in the classical age, in the Middle Ages and in the Renaissance.
The two talks by legal experts focus on cyber security and the difficult balance between fundamental rights and security needs.

Ce volume, rassemblant les contributions présentées lors de notre conférence *"De Cifris Eruditorum 2024"*, offre une analyse multidisciplinaire de la cryptographie, retraçant son parcours historique et explorant, d'un point de vue juridique, ses applications et implications actuelles.
Les trois interventions historiques couvrent l'âge classique, le Moyen Âge et la Renaissance. Les deux contributions juridiques se concentrent sur la cyber sécurité et sur le délicat équilibre entre le respect des droits fondamentaux et la nécessité de sécurité.

Massimiliano Sala & Antonino Alì
Editor in Chief & Managing Editor
De Cifris Koine

Indice

Introduzione a Eruditorum ACTA 2024 2
Antonino Alì and Massimiliano Sala

Franceschi - Partenio, una disputa crittografica nel Rinascimento 5
Paolo Bonavoglia

Scrivere per nascondere, leggere per scoprire. Le origini della crittografia 24
Marco Moraglio

Epigrafi cifrate nelle chiese antiche 35
Cosimo Palma

Il nuovo framework giuridico cyber dell'Italia. La crittografia come strumento di cybersicurezza e per l'autonomia strategica nazionale 52
Marcello Albergoni

Human Rights Implications of Encryption Backdoors 59
Antonino Alì

Human Rights Implications of Encryption Backdoors

Antonino Alì

Università di Trento, Italia
antonino.ali@unitn.it

Sommario This contribution examines the human rights implications of encryption backdoors, focusing on the landmark Podchasov v. Russia case. It analyzes the tension between national security and privacy rights in the digital age, highlighting key international instruments on encryption's role in protecting human rights. It concludes by advocating for a balanced approach that respects both security needs and fundamental rights in our increasingly interconnected world.

Introduction

Historically, intelligence agencies have adopted advanced methods to meet the challenges of modern cryptography. These organisations do not work in isolation, but actively collaborate with various partners, both internal and external, to identify potential threats and overcome the most sophisticated digital defences. There are several key components to this strategy. There is certainly constant investment in cutting-edge technology, with a focus on computing power, which enables them to tackle increasingly complex cryptographic algorithms.

However, the strategy of intelligence services is not limited to mere technological improvement. A crucial aspect is the attempt to influence the global market for commercial cryptography. This approach aims to maintain control and accessibility even in a rapidly changing digital security landscape. Through these methods, intelligence agencies seek to keep pace with the evolution of privacy techniques, balancing the need for national security with the challenges posed by modern cryptographic technologies. This is done through strategic business relationships and international cooperation. At the same time, there is a strong emphasis on developing in-house expertise. Experts in this field collaborate to create innovative approaches to cryptographic analysis. The aim is to stay one step ahead of the most robust cryptographic available technologies[1].

De Cifris Koine – Eruditorum ACTA 2024 – https://doi.org/10.69091/koine/vol-3-E05

[1] See the document "NSA's SIGINT Strategy, 2012-2016" [26]. The strategy contains objectives that underline the NSA's strategic interest in countering the challenges of cryptography to its signal intelligence missions [14, 27].

The question of weakening encryption is a classic dilemma between security and freedom, which has been exacerbated in the digital age. On the one hand, government authorities and law enforcement agencies argue that they need access to encrypted communications to counter national security threats, fight organised crime and protect children from online abuse. On the other hand, cybersecurity experts [1], digital rights advocates and much of the technology industry warn that compromising the integrity of encryption systems would pose far greater risks to collective and individual security. The essence of the dilemma lies in the primary function of robust cryptography: when implemented effectively, it prevents unauthorised access to communications, without distinguishing between malicious parties and government authorities [24].

The use of backdoors in encryption

At a time when digital security is at the centre of public debate, proposals to weaken encryption are gaining increasing attention. These initiatives, which include the introduction of 'backdoors' (a hidden function that bypasses normal security measures and allows unauthorised access to encrypted data) or the requirement for companies to retain decryption keys, aim to create exceptions to the principle of secure digital communications and attempt to strike an often precarious balance between citizens' privacy and the needs of public safety and national security. [2]

[2] The Crypto AG case, revealed in 2020, shows how hardware backdoors are used for large-scale espionage. Operation Rubicon, carried out by the CIA and BND, allowed encryption devices sold by Crypto AG to over 120 countries to be manipulated, allowing intelligence agencies to decipher the secret communications of many governments [22, 18]. Similarly, the case of the Dual_EC_DRBG algorithm, proposed by the NSA for use in the public sector, emerged in 2006. In 2007, two Microsoft researchers discovered that the algorithm could contain a backdoor, potentially allowing those who knew its details to predict its output and compromise the security of encrypted communications. Both cases highlight how backdoors, both hardware and software, can be exploited for large-scale espionage activities, raising serious concerns about the security and privacy of global communications [7]. Moreover, the case of the Clipper chip in the US in the 1990s illustrates well the debate on 'state backdoors' in encryption systems. This chip, developed at the request of government authorities, contained the Skipjack algorithm that allowed access to encrypted data in case of need. Despite the security measures provided, such as a unique serial number and a legal access unit, the project attracted strong criticism. The main concerns were the potential vulnerabilities introduced by the backdoor, the difficulty of implementing such systems securely, and the implications for privacy and data sovereignty. These concerns, combined with a lack of industry acceptance, led to the abandonment of the project. The Clipper chip case highlights the challenges and risks associated with introducing backdoors into security systems, even when requested by government authorities.

The basic idea, which may seem reasonable at first glance, is to allow authorities to access encrypted data by bypassing the encryption itself. However, when you dig deeper, there are critical issues that deserve careful consideration, especially when you consider the potential long-term implications. From a technical perspective, introducing deliberate vulnerabilities into cryptographic systems is a minefield of risks. Strong cryptography, based on mathematical algorithms so complex that even experts' heads spin, makes it virtually impossible to decipher a message without the right key. Weakening these systems, whether by using simpler keys or less secure algorithms, would be like leaving your front door open: not only could the authorities break in, but thieves and attackers could also find their way in.

Implementing secure backdoors is a tricky business, even for the most brilliant cryptographers. If designed with the best of intentions to be accessible only to authorized authorities, these vulnerabilities could still be discovered and exploited by others, creating a veritable digital Pandora's box. It is a thought-provoking paradox: in an attempt to grant access to the relevant authorities, the entire integrity of cryptographic systems may be compromised, exposing millions of users to unpredictable risks. In an increasingly interconnected world, where digital borders are as fluid as water, weakening encryption in a country could have a global impact on digital security. It is like throwing a stone into a pond: the ripples would spread far beyond the initial point of impact. And let us not forget the more sophisticated users, including potential criminals, who could simply jump into another boat, towards alternative encryption solutions and defeating, at least in part, the original purpose of the restrictions. The consequences of such a weakening are not merely technical, but extend like tentacles into the social and economic fabric. Confidence in secure digital communications is the pillar on which entire sectors, from e-commerce to financial services, rest. Compromising this trust would be like removing the foundations of a building: the impact on digital economy may be devastating [8].

The existence of backdoors, even as a possibility, could undermine user confidence in cryptographic systems and create a climate of suspicion and paranoia. The knowledge that private communications can be accessed by government authorities, even in compliance with legal procedures, could discourage the widespread adoption of encryption, much as if people stopped speaking freely for fear of being overheard.

Finally, we must not forget those for whom strong encryption is not a luxury but a vital necessity. Journalists, activists and other vulnerable groups depend on these systems to operate securely, often in contexts where their own safety is at risk. For them, weakening encryption could mean the difference between being able to do their work safely and being exposed to real and tangible dangers.

While authorities' concerns about the misuse of cryptography are understandable, experts believe that the risks of weakening cryptography outweigh the potential benefits. The challenge for the future will be to find a balance that allows legitimate security concerns to be addressed without compromising the fundamental integrity of encryption systems, which are essential for security and privacy in the digital age.

Ultimately, while backdoors appear to be a pragmatic solution to reconcile different needs, their use raises significant concerns about the overall security of systems and user trust, and requires a careful assessment of risks and benefits.

No backdoor for surveillance: ECHR protects encryption

The increasing *normalisation* of electronic surveillance,[3] and the resulting defensive countermeasures, is a phenomenon of great significance in the contemporary digital age [2]. A turning point was the revelations by Edward Snowden in 2013, which brought to light the scope and depth of surveillance activities carried out by American and British intelligence agencies. These revelations set off a chain reaction in both the technology sector and civil society[4]. The widespread adoption of end-to-end (E2E) encryption is an important response to the normalisation of surveillance [16]. Several major companies have implemented this technology for their messaging and video calling services. Some have extended end-to-end encryption to all message exchanges on their platforms, while others enhanced the security of their email services by introducing new features to increase the confidentiality of communications, although metadata generally remains accessible to the platforms.

The trend towards increased security has also led to tensions with government authorities. In the US, for example, the FBI has repeatedly raised concerns about 'going dark', arguing that strong encryption hinders legitimate investigations.[5] This fuelled debates about 'backdoors' in encryption systems, an idea strongly contested by technology companies and privacy activists.

[3] *Normalisation of surveillance* refers to the process of gradual integration of mass surveillance practices into legal and social frameworks. The European Court of Justice has, through a series of rulings, established the legality of 'bulk data collection' under certain conditions, to prevent abuses of power. The legality of such practices has specific requirements, including: clear and accessible legal basis, proportionality and necessity of the measure, independent supervision and procedural safeguards for individual rights. These rulings created a legal framework that, while recognising the potential utility of mass surveillance, seeks to balance it with the protection of citizens' rights [17, 10, 28].

[4] For an overview of cryptography and human rights issues see [25].

[5] The Apple case related to the 2016 San Bernardino massacre highlighted the complex balance between national security and privacy. When the FBI asked Apple to unlock the phone of one of the attackers, the company objected (see [3]). Apple argued that circumventing the encryption on its devices was not only technically impossible, but creating a backdoor would compromise their security. This position reflected Apple's broader concern for user privacy. Although the FBI eventually managed to unlock the phone, the case reignited the debate about government access to strong encryption. This episode showed the ongoing tension between the investigative needs of law enforcement and the need to protect the privacy of users of encrypted technologies, raising crucial questions about the future of digital security and individual rights [23].

The 'Telegram' case

A recent ruling by the European Court of Human Rights raises fundamental questions about the delicate balance between national security and individual rights to privacy and freedom of expression in the digital age. Telegram, an instant messaging application known for its emphasis on privacy and security through encryption, found itself at the centre of a legal dispute with the Federal Security Service of the Russian Federation (FSB).

The conflict arose when the FSB demanded that Telegram provide the data necessary to decrypt the communications of certain users suspected of involvement in terrorist activities. Telegram resisted these requests, claiming that providing such 'encryption keys' would compromise the security and privacy of all users of the application. In response to Telegram's refusal, the Russian authorities imposed fines and ordered the application to be blocked on Russian territory.

The dispute takes place in a complex legal context. The legislation of the Russian Federation, in particular the Information Law and subsequent decrees, imposes significant obligations on Internet communication organisations (ICOs). These include the storage of communications data on Russian territory, the transmission of such data to the competent authorities upon request, and the provision of information necessary for the decryption of encrypted electronic communications. Anton Valeryevich Podchasov, a Telegram user, had filed his application against the Russian Federation with the European Court of Human Rights (ECHR) on 18 June 2019, after exhausting domestic remedies in Russia. This was almost three years before Russia's withdrawal from the Council of Europe and the ECHR. Podchasov, along with 34 other individuals, challenged a disclosure order issued by the Russian Federal Security Service (FSB) requiring Telegram to provide technical information to decrypt the communications of users suspected of terrorist activity. The plaintiffs argued that providing the encryption keys would allow the FSB to decrypt the communications of all Telegram users, thereby violating the right to privacy and confidentiality of communications. Furthermore, they argued that once the FSB obtained the keys, it would be able to access all communications without the judicial authorisation required under Russian law.

On 25 February 2022, the Committee of Ministers of the Council of Europe suspended Russia's right of representation in the organisation, considering the aggression against Ukraine to be a serious breach of its statutory obligations. On 15 March 2022, Russia officially notified the Secretary General of the Council of Europe of its withdrawal from the organisation under Article 7 of the Statute and of its 'intention' to denounce the ECHR. The following day, 16 March 2022, the Committee of Ministers decided to expel Russia with immediate effect, despite its notification of withdrawal.

The expulsion of Russia from the Council of Europe on 16 March 2022, following the invasion of Ukraine, began the process of ending Russia's membership of the ECHR. However, a six-month transitional period was established, from 16 March to 16 September 2022,[6] during which the ECHR retained jurisdiction over cases against Russia relating to events that had occurred by the end of that period. On 5 September 2022, the plenary session of the ECHR formalised this principle, stating that the Court would retain jurisdiction to hear applications against Russia in respect of acts or omissions occurring up to 16 September 2022.[7]

The events at the centre of the Podchasov case, including the adoption of the contested law and the specific actions of the Russian authorities, occurred before 16 September 2022 and thus fall within the temporal jurisdiction of the Court. Both the Russian Government and the applicant had already submitted observations on the case before Russia's withdrawal from the ECHR, enabling the Court to proceed with its assessment.

The 'Yarovaya' Law of the Russian Federation and the obligations of 'Internet Communication Organisers' ICO

In recent years, Russia has made significant changes to its information legislation, with a particular focus on online communications.

In 2014, the Federal Law on Information, Information Technology and Information Protection was substantially amended. It introduced the concept of Internet communications organisations (ICOs), which are broadly defined to include virtually any entity that operates systems or programs for electronic communications over the Internet. The responsibilities imposed on ICOs are considerable and have a profound impact on online privacy. At the heart of the Act are its data retention requirements: ICOs must retain the metadata of user communications for a full year. This metadata includes information such as the time, date and duration of the communications, as well as the parties involved, but not the actual content of the messages. In parallel, the Act requires ICOs to retain the actual content of all communications for six months. This includes text, voice recordings, images and any other type of content exchanged by users.

[6] According to the prevailing interpretation of Article 58 of the Convention, the ECHR continued to apply to Russia for a period of six months after it ceased to be a member of the Council of Europe, thus until 16 September 2022.

[7] See the critical remarks of [5]. The Author points out that this expulsion decision raises some legal questions, as Article 8 of the Council of Europe Statute provides for a specific procedure for expulsion, which does not seem to have been fully respected.

These provisions raise important questions about the protection of privacy and freedom of online communication in Russia.[8] Indeed, the law requires ICOs to provide the authorities with the information necessary to decrypt encrypted communications, essentially requiring them to compromise the security of their systems and hand over decryption keys upon request. The technical implications of the Russian law are significant. ICOs must not only ensure that their equipment meets specific technical requirements set by the government, but also that it facilitates the work of the authorities. In practice, this could mean the integration of surveillance technologies directly into the communications infrastructure. For instant messaging services, the restrictions are even more stringent. In addition to all other requirements, these services must identify their users by their mobile phone numbers. This provision makes anonymous use of such platforms virtually impossible, raising further concerns about privacy and freedom of expression.

As reported, a particularly controversial aspect of the law is the requirement for ICOs to provide decryption keys to authorities on request. This means that in the case of encrypted communications, companies will have to provide the means to decrypt that data, raising serious concerns about user privacy and the overall security of communications systems.

The law has been presented as an anti-terrorism and national security measure aimed at assisting law enforcement and security services in their activities to prevent and investigate crime and terrorism. However, the obligation to provide decryption keys was widely perceived as a direct threat to end-to-end encryption and the confidentiality of private communications. Many industry players found it technically difficult, if not impossible, to comply with the law without compromising the security of the overall communications system. This technical difficulty highlighted the conflict between national security needs and the protection of digital privacy.

It was in this complex context that the Podchasov v. Russia case arose, which led the European Court of Human Rights to assess the compatibility of such measures with the right to privacy guaranteed by the European Convention on Human Rights. This case has become central to the debate on the regulation of encryption and the protection of personal data in the digital age.

[8] See the English text of [9].

The reasoning of the Court

In Podchasov v Russia, the European Court of Justice refers to several international instruments that underline the importance of cryptography in the context of human rights and digital security. These instruments form a coherent framework that highlights the crucial role of cryptography in protecting privacy and freedom of expression in the digital age. The 2022 report of the UN High Commissioner for Human Rights [21] emerges as a key pillar in this discussion.[9] It portrays cryptography not only as a technical tool, but as a real guarantor of fundamental rights. The report emphasises how encryption is essential to allow people to communicate freely, without fear that their information may be intercepted or misused. Particularly relevant is its warning against government restrictions on encryption, highlighting how such measures can have disproportionately negative effects on the entire population.

This view is reinforced by the 2012 Recommendation of the Committee of Ministers of the Council of Europe, which specifically encourages the use of end-to-end encryption in social networking services. This document emphasises the importance of actively protecting the privacy of online users and recognises encryption as a key tool in this endeavour.

[9] See also [15]; in this report by the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, the fundamental importance of encryption and anonymity in the digital age to ensure human rights, in particular freedom of expression and privacy, is emphasised. The paper highlights how encryption and anonymity provide the necessary security for people to freely express their opinions online without fear of retaliation or surveillance. These tools are considered essential not only for freedom of expression, but also for other rights such as privacy, due process, freedom of peaceful assembly and association, and even the right to life and physical integrity. The report strongly criticises the restrictions imposed by some states on the use of online encryption and anonymity. It points out that such restrictions often fail to meet the criteria of necessity and proportionality required by international human rights law. In particular, practices such as general bans on encryption, the intentional weakening of security standards, cryptographic key deposit systems and the requirement to disclose decryption keys are condemned. The Special Rapporteur recommends that states adopt policies that promote and protect the use of encryption and anonymity, limiting restrictions only to specific cases and on the basis of judicial orders. It emphasises the importance of a transparent public debate on any legislative proposals that would restrict the online security of individuals. The report also calls on international organisations, the private sector and civil society to actively promote the use of secure communication tools. In particular, it urges the UN system to improve its communication practices to ensure the safety of those interacting with the organisation. Finally, the document emphasises the importance of educating the public on the use of these digital security tools. The Special Rapporteur encourages states, civil society organisations and companies to engage in campaigns to promote the widespread adoption of encryption and provide the necessary tools for those at risk to securely exercise their right to freedom of opinion and expression. See also [6].

The 2015 Resolution of the Parliamentary Assembly of the Council of Europe adds a further dimension to this debate, expressing concern about the practices of some intelligence services that seek to create or exploit weaknesses in security systems. The resolution highlights the risks associated with weakening encryption, not only for individual privacy, but also for collective security against threats such as terrorism and cybercrime [4].

The Court also cites some well-known rulings of the Court of Justice of the European Union on the protection of privacy in electronic communications [19, 20]. These decisions emphasise that generalised access to the content of electronic communications is incompatible with the fundamental rights guaranteed by the EU Charter of Fundamental Rights. The 2016 Joint Statement of Europol and ENISA offers a practical perspective, recognising the need to balance investigative needs with privacy protection [12, 13]. This document advises against the introduction of mandatory backdoors or key escrow systems, emphasising how such measures can weaken overall security and be easily circumvented by criminals. Finally, the recent joint EDPB-EDPS Opinion of 2022 further reinforces the importance of encryption, warning against measures that could discourage its use [11]. This opinion emphasises how the weakening of encryption could have negative effects not only on privacy, but also on freedom of expression and digital innovation.

Overall, these instruments express a consensus on the importance of cryptography as an essential tool for the protection of human rights in the digital age. They emphasise the need for a balanced approach that respects both public security needs and the fundamental rights of citizens, and highlight the risks associated with policies that could weaken encryption. These references also show how the Court based its decision on a wide range of international sources, recognising the importance of encryption and the protection of privacy in today's digital context.

Data retention measures and the obligation to provide decryption keys

The Court found that the law violated Article 8 of the European Convention on Human Rights, which protects the right to privacy and correspondence, on three main grounds. The indiscriminate retention of data on all internet users is an "exceptionally wide and serious interference" with privacy. Adequate safeguards against abuse of data access by authorities are lacking. The obligation to decrypt end-to-end encrypted communications is disproportionate. In particular, the Court stressed that weakening encryption for all users in order to allow access by the authorities would 'seriously compromise the security of electronic communications of all users'.

This ruling is a significant victory for digital privacy, establishing that strong encryption is essential to protect fundamental rights in the digital age. The Court recognised that there are alternative methods of investigation that are less intrusive.

The issue of bulk collection of data is closely linked to the issue of encryption in Podchasov v Russia. The European Court of Human Rights recognised that the data retention measures and the obligation to provide decryption keys under Russian law constitute a de facto form of mass surveillance. Encryption, especially end-to-end encryption, is seen as a crucial defence against indiscriminate surveillance. Forcing service providers to weaken encryption or provide backdoors is tantamount to enabling mass surveillance on a large scale, compromising the privacy of all users, not just those under investigation.

The Court stressed that the indiscriminate retention of data and potential access to all encrypted communications constituted an overbroad and serious interference with the private life of individuals. This approach was considered disproportionate to the legitimate objectives of national security and crime prevention. In paragraph 70, the Court highlights the extent and gravity of the interference caused by the challenged legislation. The law provides for the automatic and continuous retention of the content of all Internet communications for six months and of related data for one year. The Court emphasises that this measure affects all users of Internet communications, irrespective of any suspicion of criminal activity, and covers the content of all communications without any limitation in terms of territorial or temporal scope or categories of persons. In paragraph 77, the Court addresses the problem of the weakening of encryption. It stresses that in order to decrypt communications protected by end-to-end encryption, such as those of Telegram, it would be necessary to weaken the encryption for all users. This cannot be limited to certain individuals and would affect everyone indiscriminately. The Court concludes that weakening encryption by creating 'backdoors' would make routine, general and indiscriminate surveillance of personal electronic communications technically possible and would seriously undermine the security of all users.

Conclusions

The decision of the European Court of Human Rights (ECHR) in Podchasov v. Russia has indeed set an important precedent for the debate on digital privacy and national security in Europe. In this case, the ECHR condemned Russia for violating the European Convention on Human Rights through its surveillance activities and failure to protect digital privacy.

This ruling has several important implications. It reaffirms the primacy of human rights and freedom of communication over national security concerns and calls on Council of Europe member states to protect these rights even when operating in the security sphere. The key role of strong cryptography in protecting privacy and digital security is clearly recognised, sending a clear message against legislative trends that aim to weaken cryptographic systems.

The Court stresses the importance of striking a balance between national security needs and respect for fundamental rights. It urges states to adopt proportionate and targeted approaches in the fight against crime and terrorism and discourages the use of generalised forms of surveillance that violate the rights to privacy and freedom of communication. This judgment marks a turning point in the protection of digital rights in Europe and provides a solid legal basis for future developments in technology and legislation.

Riferimenti bibliografici

1. H. Abelson, R. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, M. Green, S. Landau, P. G. Neumann, R. L. Rivest, J. I. Schiller, B. Schneier, M. Specter, and D. J. Weitzner. Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communication. In *Enigma 2016*. USENIX Association, 2016. https://www.schneier.com/wp-content/uploads/2016/09/paper-keys-under-doormats-CSAIL.pdf?ref=hackernoon.com.
2. A. Alì. La sorveglianza elettronica su vasta scala per finalità di intelligence nella giurisprudenza della Corte europea dei diritti dell'uomo. *La Comunità Internationale*, 1:101–115, 2022.
3. Apple. Customer letter, February 2016. https://www.apple.com/customer-letter/.
4. Parliamentary Assembly. Resolution 2045 (2015), 2015. https://pace.coe.int/files/21692/pdf.
5. L. Borlini. L'espulsione della federazione russa dal Consiglio d'Europa e le conseguenze giuridiche della cessazione della qualità di membro. *Rivista di Diritto Internazionale*, 1:37–76, 2023.
6. UCI Law International Justice Clinic. Selected References: Unofficial Companion to Report of the Special Rapporteur (A/HRC/29/32) on Encryption, Anonymity and the Freedom of Expression, 2015. https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Communications/States/Selected_References_SR_Report.pdf.
7. C. Comella. Alcune considerazioni sugli aspetti tecnologici della sorveglianza di massa, a margine della sentenza Safe Harbor della Corte di giustizia dell'Unione Europea. In G. Resta and Z. Zencovich, editors, *La protezione transnazionale dei dati personali. Dai "safe harbour princples" al "privacy shield"*, pages 49–71. Romatre-Press, Rome, 2016.
8. K. W. Dam and H. S. Lin. Cryptography's Role in Securing the Information Society. *National Academy Press*, 1996. https://nap.nationalacademies.org/read/5131/chapter/1.
9. State Duma and Federation Council. Federal Law No. 149-FZ of 27 July 2006 on Information, Information Technology and Protection of Information (as amended), July 2006. https://www.wipo.int/edocs/lexdocs/laws/en/ru/ru126en.pdf.
10. Grand Chamber European Court of Human Rights. Big Brother Watch and Others v. The United Kingdom, 2021. https://hudoc.echr.coe.int/fre?i=001-210077.
11. European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS). Joint Opinion on the Regulation of the European Parliament and of the

Council on Addressing the Dissemination of Terrorist Content Online, July 2022. https://www.edpb.europa.eu/system/files/2022-07/edpb_edps_jointopinion_202204_csam_en_0.pdf.
12. European Union Agency for Cybersecurity (ENISA). On Lawful Criminal Investigation that Respects 21st Century Data Protection, 2016. https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/on-lawful-criminal-investigation-that-respects-21st-century-data-protection.
13. Europol. On Lawful Criminal Investigation Respecting 21st Century Data Protection, 2016. https://www.europol.europa.eu/cms/sites/default/files/documents/on_lawful_criminal_investigation_respecting_21st_century_data_protection_1.pdf.
14. David P. Fidler, editor. *The Snowden Reader*. Indiana University Press, Bloomington, IN, 2015.
15. D. Kaye. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. *Human Rights Council, Twenty-ninth Session*, 2015. https://daccess-ods.un.org/access.nsf/Get?OpenAgent&DS=A/HRC/35/22&Lang=E.
16. R. Lakra. Cracking the Code: How Podchasov v. Russia Upholds Encryption and Reshapes Surveillance. *EJIL: Talk*, March 2024. https://www.ejiltalk.org/cracking-the-code-how-podchasov-v-russia-upholds-encryption-and-reshapes-surveillance/.
17. M. Milanovich. The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för Rättvisa. *EJIL: Talk!*, 2021. https://www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa/.
18. G. Miller. How the CIA Used Crypto AG Encryption Devices to Spy on Countries for Decades. *Washington Post*, February 2020. https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/.
19. Court of Justice of the European Union. Judgment of the Court of Justice of the European Union in the Joined Cases of Digital Rights Ireland and Seitlinger and Others. case C-293/12 and C-594/12 (EU:C:2014:238), 2014.
20. Court of Justice of the European Union. Judgment of the Court of Justice of the European Union in the Case of Maximillian Schrems v. Data Protection Commissioner. case C-362/14 (EU:C:2015:650), 2015.
21. Office of the United Nations High Commissioner for Human Rights. The Right to Privacy in the Digital Age. *Human Rights Council, Fifty-first Session*, 2022. https://daccess-ods.un.org/access.nsf/Get?OpenAgent&DS=A/HRC/51/17&Lang=E.
22. Parliament of the Swiss Confederation. Affaire Crypto AG: Rapport de la Délégation des Commissions de gestion des Chambres fédérales, November 2020. https://www.parlament.ch/centers/documents/fr/bericht-gpdel-2020-11-10-f.pdf.
23. M. Sala. La Crittografia al centro dello scontro tra Apple ed FBI. *Gnosis*, 2:139–143, 2015. https://gnosis.aisi.gov.it/Gnosis/rivista47.nsf/servnavig/47-39.pdf/$File/47-39.pdf?OpenElement.
24. B. Schneier. The Value of Encryption. The Ripon Forum, 2016. https://www.schneier.com/essays/archives/2016/04/the_value_of_encrypt.htm.

25. W. Schulz and J. van Hoboken, editors. *Human Rights and Encryption*. UNESCO Internet Freedom Series. UNESCO Publishing, 2016. https://www.hiig.de/wp-content/uploads/2016/12/246527E.pdf.
26. New York Times. A Strategy for Surveillance Powers, 2013. https://archive.nytimes.com/www.nytimes.com/interactive/2013/11/23/us/politics/23nsa-sigint-strategy-document.html.
27. U.S. House of Representatives. Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden. Technical report, U.S. Government Printing Office, 2016. https://www.congress.gov/114/crpt/hrpt891/CRPT-114hrpt891.pdf.
28. E. Watt. *State Sponsored Cyber Surveillance: The Right to Privacy of Communications and International Law*. Edward Elgar Publishing, Cheltenham, 2021.