VI CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL (VI CIDIA)

PRIVACIDADE, PROTEÇÃO DE DADOS PESSOAIS E NEGÓCIOS INOVADORES I

P961
Privacidade, proteção de dados pessoais e negócios inovadores II [Recurso eletrônico on-line] organização VI Congresso Internacional de Direito e Inteligência Artificial (VI CIDIA): Skema Business School – Belo Horizonte;

Coordenadores: Alexandre Schmitt da Silva Mello, Mariana de Moraes Palmeira e Pietra Daneluzzi Quinelato – Belo Horizonte: Skema Business School, 2025.

Inclui bibliografia
ISBN: 978-65-5274-361-9
Modo de acesso: www.conpedi.org.br em publicações
Tema: Perspectivas globais para a regulação da inteligência artificial.
1. GDPR. 2. Segurança da informação. 3. Compliance. I. VI Congresso Internacional de Direito e Inteligência Artificial (1:2025 : Belo Horizonte, MG).

CDU: 34

VI CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL (VI CIDIA)

PRIVACIDADE, PROTEÇÃO DE DADOS PESSOAIS E NEGÓCIOS INOVADORES I

Apresentação

A SKEMA Business School é uma organização francesa sem fins lucrativos, com presença em sete países diferentes ao redor do mundo (França, EUA, China, Brasil, Emirados Árabes Unidos, África do Sul e Canadá) e detentora de três prestigiadas acreditações internacionais (AMBA, EQUIS e AACSB), refletindo seu compromisso com a pesquisa de alta qualidade na economia do conhecimento. A SKEMA reconhece que, em um mundo cada vez mais digital, é essencial adotar uma abordagem transdisciplinar.

Cumprindo esse propósito, o VI Congresso Internacional de Direito e Inteligência Artificial (VI CIDIA), realizado nos dias 18 e 19 de setembro de 2025, em formato híbrido, manteve-se como o principal evento acadêmico sediado no Brasil com o propósito de fomentar ricas discussões sobre as diversas interseções entre o direito e a inteligência artificial. O evento, que teve como tema central a "Regulação da Inteligência Artificial", contou com a presença de renomados especialistas nacionais e internacionais, que abordaram temas de relevância crescente no cenário jurídico contemporâneo.

Profissionais e estudantes dos cursos de Direito, Administração, Economia, Ciência de Dados, Ciência da Computação, entre outros, tiveram a oportunidade de se conectar e compartilhar conhecimentos, promovendo um ambiente de rica troca intelectual. O VI CIDIA contou com a participação de acadêmicos e profissionais provenientes de diversas regiões do Brasil e do exterior. Entre os estados brasileiros representados, estavam: Alagoas (AL), Bahia (BA), Ceará (CE), Goiás (GO), Maranhão (MA), Mato Grosso do Sul (MS), Minas Gerais

Foram discutidos assuntos variados, desde a própria regulação da inteligência artificial, eixo central do evento, até as novas perspectivas de negócios e inovação, destacando como os algoritmos estão remodelando setores tradicionais e impulsionando a criação de empresas inovadoras. Com uma programação abrangente, o congresso proporcionou um espaço vital para discutir os desafios e oportunidades que emergem com o desenvolvimento algorítmico, reforçando a importância de uma abordagem jurídica e ética robusta nesse contexto em constante evolução.

A programação teve início às 13h, com o check-in dos participantes e o aquecimento do público presente. Às 13h30, a abertura oficial foi conduzida pela Prof.ª Dr.ª Geneviève Poulingue, que, em sua fala de boas-vindas, destacou a relevância do congresso para a agenda global de inovação e o papel da SKEMA Brasil como ponte entre a academia e o setor produtivo.

Em seguida, às 14h, ocorreu um dos momentos mais aguardados: a Keynote Lecture do Prof. Dr. Ryan Calo, renomado especialista internacional em direito e tecnologia e professor da University of Washington. Em uma conferência instigante, o professor explorou os desafios metodológicos da regulação da inteligência artificial, trazendo exemplos de sua atuação junto ao Senado dos Estados Unidos e ao Bundestag alemão.

A palestra foi seguida por uma sessão de comentários e análise crítica conduzida pelo Prof. Dr. José Luiz de Moura Faleiros Júnior, que contextualizou as reflexões de Calo para a realidade brasileira e fomentou o debate com o público. O primeiro dia foi encerrado às 14h50 com as considerações finais, deixando os participantes inspirados para as discussões do dia seguinte.

As atividades do segundo dia tiveram início cedo, com o check-in às 7h30. Às 8h20, a Prof.ª Dr.ª Margherita Pagani abriu a programação matinal com a conferência Unlocking Business Creativity Using Artificial Intelligence, apresentando insights sobre como a IA pode

Após um breve e merecido coffee break às 9h40, os participantes retornaram para uma manhã de intensas reflexões. Às 10h30, o pesquisador Prof. Dr. Steve Ataky apresentou a conferência Regulatory Perspectives on AI, compartilhando avanços e desafios no campo da regulação técnica e ética da inteligência artificial a partir de uma perspectiva global.

Encerrando o ciclo de palestras, às 11h10, o Prof. Dr. Filipe Medon trouxe ao público uma análise profunda sobre o cenário brasileiro, com a palestra AI Regulation in Brazil. Sua exposição percorreu desde a criação do Marco Legal da Inteligência Artificial até os desafios atuais para sua implementação, envolvendo aspectos legislativos, econômicos e sociais.

Nas tardes dos dois dias, foram realizados grupos de trabalho que contaram com a apresentação de cerca de 60 trabalhos acadêmicos relacionados à temática do evento. Com isso, o evento foi encerrado, após intensas discussões e troca de ideias que estabeleceram um panorama abrangente das tendências e desafios da inteligência artificial em nível global.

Os GTs tiveram os seguintes eixos de discussão, sob coordenação de renomados especialistas nos respectivos campos de pesquisa:

a) Startups e Empreendedorismo de Base Tecnológica – Coordenado por Allan Fuezi de Moura Barbosa, Laurence Duarte Araújo Pereira, Cildo Giolo Júnior, Maria Cláudia Viana Hissa Dias do Vale Gangana e Yago Oliveira

b) Jurimetria Cibernética Jurídica e Ciência de Dados – Coordenado por Arthur Salles de Paula Moreira, Gabriel Ribeiro de Lima, Isabela Campos Vidigal Martins, João Victor Doreto e Tales Calaza

c) Decisões Automatizadas e Gestão Empresarial / Algoritmos, Modelos de Linguagem e Propriedade Intelectual – Coordenado por Alisson Jose Maia Melo, Guilherme Mucelin e

f) Regulação da Inteligência Artificial – III – Coordenado por Ana Júlia Silva Alves Guimarães, Erick Hitoshi Guimarães Makiya, Jessica Fernandes Rocha, João Alexandre Silva Alves Guimarães e Luiz Felipe Vieira de Siqueira

g) Inteligência Artificial, Mercados Globais e Contratos – Coordenado por Gustavo da Silva Melo, Rodrigo Gugliara e Vitor Ottoboni Pavan

h) Privacidade, Proteção de Dados Pessoais e Negócios Inovadores – I – Coordenado por Dineia Anziliero Dal Pizzol, Evaldo Osorio Hackmann, Gabriel Fraga Hamester, Guilherme Mucelin e Guilherme Spillari Costa

i) Privacidade, Proteção de Dados Pessoais e Negócios Inovadores – II – Coordenado por Alexandre Schmitt da Silva Mello, Lorenzzo Antonini Itabaiana, Marcelo Fonseca Santos, Mariana de Moraes Palmeira e Pietra Daneluzzi Quinelato

j) Empresa, Tecnologia e Sustentabilidade – Coordenado por Marcia Andrea Bühring, Ana Cláudia Redecker, Jessica Mello Tahim e Maraluce Maria Custódio.

Cada GT proporcionou um espaço de diálogo e troca de experiências entre pesquisadores e profissionais, contribuindo para o avanço das discussões sobre a aplicação da inteligência artificial no direito e em outros campos relacionados.

Um sucesso desse porte não seria possível sem o apoio institucional do Conselho Nacional de Pesquisa e Pós-graduação em Direito - CONPEDI, que desde a primeira edição do evento provê uma parceria sólida e indispensável ao seu sucesso. A colaboração contínua do CONPEDI tem sido fundamental para a organização e realização deste congresso, assegurando a qualidade e a relevância dos debates promovidos.

Reitora – SKEMA Business School - Campus Belo Horizonte

Prof. Ms. Dorival Guimarães Pereira Júnior

Coordenador do Curso de Direito – SKEMA Law School

Prof. Dr. José Luiz de Moura Faleiros Júnior

Coordenador de Pesquisa – SKEMA Law School

QUEM TEM A CHAVE? UMA ANÁLISE DA CRIPTOGRAFIA COMO FERRAMENTA DE PROTEÇÃO DE DADOS PESSOAIS E COMO AUTORIDADES TENTARAM OBTER CONTROLE SOBRE ESTA TECNOLOGIA ATRAVÉS DA HISTÓRIA

WHO HOLDS THE KEY? AN ANALYSIS OF CRYPTOGRAPHY AS A TOOL TO PROTECT PERSONAL DATA AND AUTHORITIES' ATTEMPTS TO GAIN CONTROL OVER IT THROUGHOUT HISTORY

Izabela Mendonça Acorroni [1]

Resumo

O presente artigo examina o uso da criptografia como ferramenta de proteção de dados pessoais e a tentativa de autoridades em controlar referida tecnologia. Utilizando metodologia qualitativa, é traçada uma análise histórica da criptografia, examinando ações governamentais de controle durante as chamadas "guerras criptográficas". Ademais, referenciais filosóficos são utilizados para conectar tais iniciativas de controle da referida tecnologia ao poder de vigilância estatal. Conclui-se que indivíduos devem manter o direito ao uso da criptografia para a proteção da privacidade, garantindo liberdades civis e combatendo a censura.

Palavras-chave: Criptografia, Criptografia de dados, Vigilância digital, Guerras criptográficas, Privacidade

Abstract/Resumen/Résumé

This paper examines the tension surrounding the use of cryptography for individuals as a tool to protect personal data versus the authorities' pursuit of control over it. Adopting a qualitative methodological approach, it traces cryptography's history, examining government attempts to control encryption during "cryptowars". Furthermore, philosophical frameworks are used to contextualise digital surveillance, bridging authorities' efforts of cryptography control to state surveillance power. Ultimately, it concludes that individuals should maintain the right to use encryption for privacy, safeguarding civil liberties and countering censorship

Introduction

In the *onlife* world (HILDEBRANDT, 2016, p.1), the motto has changed from "knowledge is power"[1] to "data is power". When cryptography is introduced into this equation, one might argue that if data is power, information becomes the key, and whoever holds this key, holds the power. This notion becomes particularly evident when analysing the persistent efforts of authorities to gain control over encrypted information. That is why in this research, we shall examine the motivations behind authorities' pursuit of control over cryptography and question whether it is justified.

Initially, we explore cryptography within its historical context, tracing its evolution from ancient encrypted messages through the sophisticated encryption machines of the Second World War, culminating in the advent of public-key cryptography. We will then examine contemporary applications of cryptography, highlighting its role in protecting privacy and its emergence as a tool (or weapon?) of resistance. This discussion includes addressing the cryptowars and how authorities have responded to it, supported by analyses of specific real-world cases.

Subsequently, we connect the authorities' pursuit of control to state surveillance powers. Drawing upon Michel Foucault's concept of the panopticon as a starting point, we will explore how his theory extends beyond the mere concept of surveillance, to encompass a broader interpretation of power and a society of discipline. Following this, we examine Gilles Deleuze's theoretical framework concerning societies of control. To conclude this theoretical exploration, we incorporate the work of Haggerty and Ericson, who integrate and extend the theories of Foucault, Deleuze, and Guattari through their concept of the surveillance assemblage, thereby accurately reflecting the complex realities of contemporary digital societies.

To conclude, we will summarise arguments opposing governmental control of cryptography, underscoring that although cryptography possesses significant power, governments should not inherently view it as a threat. Instead, we propose that authorities should focus on regulating or controlling specific cryptographic applications related directly to national security and law enforcement, clearly delineating limits to prevent misuse.

[1] The well-known Latin saying *"scientia potentia est"*, meaning "knowledge is power", is generally credited to Sir Francis Bacon.

Ultimately, we advocate that unrestricted development and utilisation of cryptography are vital for safeguarding civil liberties and preserving individual privacy.

1 Objective

This research aims to critically examine the motivations and implications behind authorities' attempts to control cryptography throughout history, exploring its evolution, its role as a tool for resistance, and the ensuing debates about digital surveillance and privacy.

2 Methodology

For better comprehension and development of the argument of this research, a qualitative methodological approach is adopted, particularly, a descriptive treatment through literature revision and research, combining historical analysis to contextualise the progression and importance of cryptography with philosophical analysis to interpret the broader implications of surveillance mechanisms using frameworks provided by Foucault, Deleuze, Haggerty and Ericson. Through this interdisciplinary analysis, the paper seeks to provide insights into why unrestricted cryptographic practices are essential to preserve individual privacy and control of personal data.

3 Development

3.1 Evolution of cryptography: a brief history

It is hard to pinpoint exactly where the history of cryptography began, but we can trace it back to evidence of its use in early writing systems in societies such as the Egyptian, Greek, Roman, and others. These societies aimed to convey cryptographic messages through "schemes of secret writing" (DAVIES, 1997, p.14), utilising methods of transposition and substitution. The study of cryptography is believed to have started developing during the Renaissance, driven by political interests and the need to keep intercepted letters private due to their content on war, diplomacy, and other similar affairs (Ibid.). At the time, the "dominant scheme of cryptography" was the nomenclator (Ibid, p.15), a technique that combined "alphabetic cypher with a code book" (Ibid.). As technology evolved, so did cryptography, continually changing with the introduction of the telegraph and leading to the development of

complex machines in the 1920s and 1930s. This evolution culminated in the most emblematic historical case of cryptography use: the Enigma machine during the Second World War (Ibid.).

The famous Enigma machine, used by the German military, was a nightmare for the Allies in the War. It was an “electromechanical device consisting of a set of rotors or wheels with electrical contacts on each side of the rotor producing a complex substitution cypher” (LANDAU, 2013, p.44). The British expended considerable effort in cracking Enigma's codes. By establishing a “cryptanalytic centre” (DAVIES, 1997, p.16) and developing the Colossus machine – the first known electronic computer – the Allies managed to decipher a high percentage of the German military messages. This achievement is believed to have significantly contributed to their victory in the war. However, since the British did not disclose their cryptographic work until the late 2000s, after the end of WWII “the development of Government cryptology is a closed book once again” (Ibid.), with no significant outcomes until 1970.

It is an academic consensus that the year of 1970 bore “two developments that have fundamentally changed the nature of overt cryptography” (Ibid., p.17). First, the United States Government published the Data Encryption Standard (DES), driven by the necessity “to protect the sensitive civilian data that it was electronically transmitting and storing” (LANDAU, op. cit., p. 44). This action was the catalyst that led to the formal study of cryptography spreading worldwide (DAVIES, op. cit., p. 17). Shortly after this disclosure, in 1976, Whitfield Diffie and Martin Hellman proposed the concept of public-key cryptography, a method that uses a widely known public key for encryption and a private key for decryption (LANDAU, op. cit., p. 45), allowing “two parties that have not previously communicated to establish a secure communication link over an insecure channel” (Ibid., p. 46). Public-key cryptography was “the enabler of many digital things” (Ibid.), and it is still used today, most notably in HTTPS web sessions, VPN networks, and other similar applications.

3.2 When a tool can become a weapon: modern cryptography, cryptowars and the authorities response

At first, governments were not concerned about the use of encryption by the general population because the authorities held the knowledge and power over it. If someone encoded something, the authorities could easily decode it (KOOPS and COSTA, 2018, p. 893).

However, as aforementioned, the historical evolution of cryptography made this technology stronger – even unbreakable in certain cases – which led to governments worrying about its usage, as "people could use robust cryptography and the police and national security agencies stood empty-handed" (Ibid.). Additionally, there was a movement to create strong cryptography and make it available for download with open-source tools, thereby popularising its use among the general public. Koops and Kosta argue that control over cryptography started being debated under the guise of defending national security and enforcing the law (Ibid.). In the context of both aforementioned arguments, much was discussed and implemented in the early 1990s, in what Koops and Kosta call the first part of the cryptowars debate (Ibid.).

The argument of national security was particularly related to the use of cryptography by foreigners, which led to the development of international agreements regarding the export of cryptography (Ibid, p. 893). For example, in 1995 the Wassenaar Agreement, a non-binding international instrument, categorised cryptography as a "dual-use good" (Ibid.) to "allow only export of weak (easily crackable) cryptography and to require licences for export of strong cryptography" (Ibid.). The argument of enforcing the law relates to domestic uses of cryptography, which proved to be more complex. In the early 1990s, the authorities realised that "law enforcement could be seriously hampered by cryptography" (Ibid.). The proposed solution was to give authorities access beforehand, for example, stating that people need to "deposit keys somewhere when they want to use cryptography" (Ibid.); or access could be given afterward, using some backdoor mechanism (Ibid.). However, time proved that these efforts by authorities to control cryptography would not suffice in their goal, as evidenced by examples around the world.

A famous example was the Clipper chip, that the US government tried to implement in 1993. The idea consisted in "a chip for telephone encryption with a built-in backdoor for government access" (Ibid.), but faced severe opposition from privacy advocates and legal challenges, leading to the project's abandonment. The United Kingdom also participated in this movement. In the early 1990s, the government launched a series of "proposals for government backdoor access to encoded data" (Ibid., p. 894), which were reassessed and some of them abandoned a few years later, because the backdoor scheme was believed to be inconsistent and not entirely reliable, as it could not prevent people from using encryption (Ibid.). As the backdoor strategy has proven difficult to implement, a new option emerged within governments such as those of the UK, Netherlands, Belgium, France, and others: the development of legislation that would allow "the police to command people to decrypt or to

hand over their crypto keys" (Ibid.). This strategy also proved to be unfruitful, as it did not solve the main problem of unwanted use of encryption and had many loopholes in its application.

The authors also analyse the belief that the development of end-to-end encryption proved itself to be "a major obstacle in practice" (Ibid.) to the strategies adopted by governments. Snowden's revelations made it clear that governments and authorities would hijack cryptography and invade users' privacy, displaying an imbalanced power relationship. This event "raised significant awareness on the interception capabilities of intelligence services and the debate reheated around the powers of security and intelligence services and law enforcement agencies" (Ibid., p. 896). End-to-end encryption spread to companies such as Apple, WhatsApp, and Meta, and even the general public started using encryption software for private communications (Ibid.). Fighting pervasive surveillance with more encryption became the posture adopted by many. Simon Price (1999, p. 96) reminds us that in modern society, people tend to forget that cryptography "is all around us, only hidden", with its usage spread everywhere: payments, companies' systems, communication, softwares, and so on (Ibid.). However, what about surveillance?

3.3 Digital surveillance

To delve into the surveillance context, we will start by exploring Foucault's concept of surveillance. Foucault (1991, p. 198) presents us something that surpasses the simple concepts of surveillance, providing a theory of power and a society of discipline. The Panopticon extends beyond a mere architectural proposal for prisons and is applied to all of society's disciplinary institutions (schools, the military, hospitals). Foucault begins his discussion of Panopticism by analysing the instructions published in the 17th century to deal with the great plague. In doing so, he addresses the first large-scale disciplinary project in a society, where the control of every movement gave birth to the "utopia of the perfectly governed city" (Ibid.). From this disciplinary project, an architectural composition emerged: Bentham's Panopticon. The structure of the Panopticon is simple: the space is designed in a circle with a tower constructed in the middle, surrounding this tower are individual cells. The tower projects bright light in a way that allows the observer inside the tower to see the cells, but the individuals in the cells cannot see into the tower. This structure was believed to allow the induction of an automatic functioning of power (Ibid., p. 201).

The Panopticon mechanism was also a state of experimentation: by controlling the environment, one could perform experiments of many sorts. According to Foucault, "the panopticon functions as a kind of laboratory of power" (Ibid., p. 204) because it is through power that the observation of behaviour is allowed (Ibid.). More than just an architectural structure, Bentham conceived the ultimate principle of power: that it should be visible and unverifiable (Ibid.). Foucault indicates that we need to transcend its architectural definition to conceive the Panopticon as a general model that could function in any situation of power relation (Ibid., p. 205). By being a general model, it also should function to avoid the risk of tyranny by those who control power: because in each Panopticon application, the application of power is diffused, it reduces the number of those who exercise power while increasing the number of those upon whom power is exercised (Ibid., p. 206). The model of the Panopticon arises as an answer to a changing political and societal context, where the rule of the sovereign in the model of the Leviathan fails to work. Panopticism is then, according to Foucault, an answer to the emergence of a society that no longer relies on the guidance of the collective, the public life, but concerns itself with the state affairs of individuality (Ibid.). But could this theory still endure throughout time?

Deleuze (1992, p. 2), on the other hand, brings us the concept that the society of disciplines introduced by Foucault is a valid, yet outdated, concept. According to Deleuze, what started in the 19th century, and continues to endure now, is the society of control. The premise of the society of control is that it works with modulation of the individual, and we need to consider the spaces of enclosure as moulds (the school, the factory, and so on), as Deleuze says, a "self-deforming cast" (Ibid.) that transmutes and changes. Unlike disciplinary societies, these "spaces of enclosure" (Ibid.) are one big metastasis of this system of deformation. They coexist within each other, and the individual is never finished with any of them; he cannot move from one space to another because they are all intertwined. Deleuze makes unique observations by matching types of machines to types of society. Societies of sovereignty are matched with simpler machines like levers and clocks; disciplinary societies are matched with machines involving energy; and societies of control are matched with computers. According to Deleuze, the corporation is the ultimate example of the controlling society, and the dichotomy of individuality/masses in the disciplinary society gives way to "dividuals" (Ibid., p. 4).

Haggerty and Ericson (2000, p. 608) go further and unite Foucault, Deleuze, and Guattari to come up with the concept of the surveillance assemblage, defining what we experience today in modern societies. The authors invite us to delve into "a set of conceptual

tools that allow us to re-think the operation of the emergent surveillance system, a system we call the "surveillance assemblage" (Ibid). The concept of assemblage is proposed as a different way to interpret Foucault's work on surveillance, considering that assemblage represents a multiplicity of different objects that unite solely with the purpose of "working together as a functional entity" (Ibid.). Since society has become mainly deterritorialised, surveillance operates on a global scale. Adding digitalisation into the equation transforms the surveillance system into a technological one, "a process whereby it is increasingly difficult for individuals to maintain their anonymity, or to escape the monitoring of social institutions" (Ibid., p. 619). The digital surveillance assemblage thus metamorphoses into the ancient figure of the all-seeing eye, collecting information everywhere. The well-known authorities' discourse of protecting national security and enforcing the law begins to sound hollow as disclosures about how this surveillance is conducted make front-page news.

3.4 Who holds the key? When authorities' control over cryptography entangles with surveillance powers

Feigenbaum and Weitzner (2018, p. 267) discuss the approaches taken by researchers, officials and others – both in the fields of technology and law – regarding the tension that exists between encryption and surveillance. At one end, there is "the view that the technical community is simply thwarting the lawful exercise of warrants and court orders authorised by statute and the relevant basic law" (Ibid.), obliged to assist government authorities in the execution of these warrants and orders. Regarding this argument, we observe that this obligation of assistance is far from settled and "it does not fully resolve the tension between lawful surveillance and end-to-end encryption" (Ibid.). For example, in the famous FBI vs. Apple case, the requirement for Apple to write new software that would enable the government to access an iPhone was heavily debated and was not resolved in court (Ibid.). The risks a backdoor such as this promotes were numerous, due to the possibility that it could be wrongfully misused: "in the Vodafone Greece scandal for example, a wiretapping capability mandated by US Law was used against Greek government officials" (Ibid.). These examples make it evident that a general obligation of assistance based on a legal framework is too broad to address the discussions surrounding encryption and surveillance, lacking specificity regarding what can be imposed concerning encryption (Ibid., p. 268).

The second argument the authors present, at the other end of the spectrum, "is the view that governments, including democratic ones, routinely violate privacy rights" (Ibid.).

Because privacy is a fundamental right, tech developers would be “morally obligated to build user-friendly strong encryption into as much of the computing and communications infrastructure as possible” (Ibid.), with the goal to make it difficult for government authorities to decrypt anything. Snowden's revelations were a significant catalyst for this movement, which aims to counter mass surveillance with mass encryption (Ibid.). However, the authors claim that “while there is a great deal of truth in this view of the situation, it does not satisfactorily resolve the question of how to accomplish lawful surveillance in a mass-encryption world” (Ibid.). Indeed, what Feigenbaum and Weitzner are illustrating in their studies is that both approaches are at completely opposite ends of the spectrum. At this point, we should ask ourselves: Is it possible for authorities to lawfully obtain control over cryptography? We will address this question in the last section of this paper.

3.5 Relating surveillance, cryptography, privacy and censorship

We have already discussed that surveillance is a powerful mechanism of control, and as society progresses towards a digital, technologically-based world, surveillance becomes more prevalent. It is important to point out that digital surveillance by itself is not a problem – the question that needs answering is that, to exercise surveillance, the state needs to do so in a way that provides guarantees against abuse, therefore compatible with a democratic society, and frequently they fail to do so. Regarding encryption, Rogaway (2015, p. 1) cites that “cryptography rearranges power: it configures who can do what, from what. This makes cryptography an inherently political tool”. In the previously discussed historical evolution of cryptography, it became clear that as people started to use the technology, the shift of power left authorities concerned. As cryptography became unbreakable in certain cases, governments started to devise strategies to access encrypted information: using backdoors, developing legal and policy frameworks about cryptography usage and importation, usually resorting to the well-known arguments of national security and law enforcement. During the cryptowars, people were fighting back against governments by creating stronger cryptography methods and making them available to the public through open-source platforms. Cryptography proved itself to be a powerful tool to protect people's privacy when their own government was unlawfully seeking sensitive information, as shown in Snowden's revelations. This situation underscores the argument posed by this paper, namely, that the fact that cryptography became too powerful and is now in the hands of the people should not be an

argument to endorse its control by authorities, and that pervasive surveillance could be interpreted as a threat to people's privacy.

Brunton and Nissenbaum (2015, p. 45) talk about privacy as a “multi-faceted concept” that bears a “wide range of structures, mechanisms, rules, and practices available to produce it and defend it”. Cryptography is one of these mechanisms that can be found within the imaginary drawers of the privacy tool chest (Ibid.), and it becomes a weapon of resistance: to illustrate, the authors cite BlackNet, a cryptographic application whose aim was “to describe a wholly anonymous information marketplace, with untraceable transactions” (Ibid., p. 46). Obfuscation, they say, is a tool to data privacy: it is a technique of “making noise” (Ibid.) in the process of collecting data, making this data “more ambiguous, confusing, harder to exploit, more difficult to act on, and therefore less valuable” (Ibid.). The authors suggest that obfuscation is also a tool for protest, as the collection of information we face with digital surveillance “takes place in an asymmetrical power relationship” (Ibid.). After the scandal involving Snowden's revelations, the movement in favour of using cryptography to resist government pervasive surveillance became even stronger. At the time, US cryptography researchers wrote an open letter voicing their concerns over authorities wanting to control encrypted information, which reads:

> Indiscriminate collection, storage, and processing of unprecedented amounts of personal information chill free speech and invite many types of abuse, ranging from mission creep to identity theft. These are not hypothetical problems; they have occurred many times in the past. Inserting backdoors, sabotaging standards, and tapping commercial data-centre links provide bad actors, foreign and domestic, opportunities to exploit the resulting vulnerabilities (ABADI and others, 2014).

At this juncture, it is important to also comment on the argument that the control of cryptography by authorities represents an act of censorship. According to Tanczer, McConville and Maynard (2016, p. 346), “processes of eavesdropping and information collection (i.e., surveillance) are often interrelated with processes of removal, displacement, and restriction of material or speech (i.e., censorship)”. In the liberal conception, censorship is something external to the communication process, being the censor a social authority who wants to intervene and control free speech; in a repressive way (BUNN, p. 29-30). Bunn presents the idea that Foucault's work on surveillance changed the perspective of the liberal

concept of censorship, developing a new censorship theory (Ibid., p. 39). With this new conception, censorship becomes structural (Ibid.). Add technology to the equation, and digital surveillance becomes the epitome of censorship. “The encryption of data is a way to elude censorship or surveillance” (TANCZER, MCCONVILLE AND MAYNARD, op. cit., p. 350); thus, cryptography emerges as a vital tool for individuals to reclaim their privacy and freedom of speech. By encrypting their communications and data, individuals can resist the intrusive reach of authorities, effectively countering the structural censorship embedded within pervasive surveillance.

However, we still need to point out that even in democratic countries, the use of strong cryptography may not guarantee the user's privacy on their communication. Keenan (2019, p. 1) shows us that, historically, the United Kingdom has a long and complicated history regarding interception of communication intertwined with surveillance power. Regarding the UK access to encrypted data the legal framework can be extensive, going through interception warrants, the Investigatory Powers Act, the Terrorist Act and more (Ibid.). In a bold manoeuvre, Government Communications Headquarters officials even suggested that “rather removing encryption, the software on a targeted device should be secretly modified so as to copy all targeted communications to GCHQ” (Ibid., p.9). This shocking proposal was the stage of strong debates of “privacy advocates and technology companies” (Ibid.) who wrote an open letter stating that the proposal undermined authentication, destroyed systemic trust, created risks of exposing the platform to vulnerabilities, and opened precedents to other countries to access encrypted information (Ibid., p. 11). This last example exposes what we constructed as our argument throughout this paper: people should not be denied the right to privacy by using encryption and should not be compelled to disclose encrypted information. The power imbalance that exists in the government-citizens relationship cannot be enhanced through pervasive surveillance, and when authorities are dealing with real threats regarding national security and law enforcement, they should aim measures towards other issues that are not indiscriminate control over cryptography.

4 Conclusion

In conclusion, it became clear that cryptography can perform a power shift between individuals and authorities, and that this is something governments’ fought to keep control throughout history. As we contemplated the history of cryptography, we delved into the development of the technology since ancient times to modern uses, and catalogued some

initiatives governments tried to implement throughout the years: using backdoors, developing legal and policy frameworks about cryptography usage and importation, always recurring to the arguments of national security and law enforcement. However, we pointed out that these arguments often hide the true desire of authorities to control encrypted information: to perform surveillance.

At this point, we ventured into the notion of surveillance, starting to trace a philosophical approach of the term by Foucault's panopticon and the concept of the society of discipline. We counterargue Foucault with Deleuze's society of control, a concept more fitting to what we experienced after the 19th century. However, as modern society develops and faces the digital world, we pointed out that Haggerty and Ericson go further and unite Foucault, Deleuze, and Guattari to come up with the concept of the surveillance assemblage, defining what we experience today in modern digital societies. Digital surveillance then emerges as a powerful force utilised by governments, and we reaffirmed that the real problem lies in the pervasive surveillance.

The research shows that cryptography proved itself to be a powerful tool to protect people's privacy when their own government was unlawfully seeking sensitive information, as shown in Snowden's revelations. This situation underscores the argument posed by this essay, namely, that the fact that cryptography became too powerful and is now in the hands of the people should not be a reason to endorse its control by authorities. In fact, we showed that the control over cryptography with surveillance purposes can be interpreted as censorship and a threat to people's privacy.

References

ABADI, M. *et al.* **An Open Letter from US Researchers in Cryptography and Information Security.** 24 jan. 2014. Disponível em: http://masssurveillance.info. Acesso em: 9 maio 2025.

BRUNTON, F.; NISSENBAUM, H. Why is obfuscation necessary? *In:* BRUNTON, F.; NISSENBAUM, H. **Obfuscation: A User's Guide to Privacy and Protest.** Cambridge: MIT Press, 2015. cap. 3, p. 45-62.

BUNN, M. Reimagining Repression: New Censorship Theory and After. **History and Theory**, v. 54, n.1, p. 25-44. 2015.

DAVIES, D. A Brief History of Cryptography. **Information Security Technical Report**, v. 2, n. 2, p. 14-17. 1997.

DELEUZE, G. Postscript on the Societies of Control. **MIT Press**, Cambridge, v. 59, p. 3-7. 1992.

FEIGENBAUM, J.; WEITZNER, D. J. On the Incommensurability of Laws and Technical Mechanisms: Or, What Cryptography Can't Do. *In:* MATYÁŠ, V. *et al*. (org.) **Security Protocols 2018: Lecture Notes in Computer Science**. Cambridge: Springer, 2018. cap. XXVI, p. 280-288.

FOUCAULT, M. Panopticism. *In:* **Discipline and Punish: The Birth of the Prison.** London: Penguin Books, 1991. cap. 3, p. 195-228.

HAGGERTY, K. D.; ERICSON, R. V. The Surveillance Assemblage. **British Journal of Sociology**, London, v. 51, n. 4, p. 605-622. 2000.

KEENAN, B. State access to encrypted data in the United Kingdom: The "transparent" approach. **Common Law World Review**, v. 49, n. 3-4, p. 223-244. 2019.

KOOPS, B.-J.; KOSTA, E. Looking for some light through the lens of "cryptowar" history: Policy options for law enforcement authorities against "going dark." **Computer Law & Security Review**, v. 34, n. 4, p. 890-900. 2018.

LANDAU, S. Securing the Internet is Difficult. *In:* **Surveillance or Security? The Risks Posed by New Wiretapping Technologies**. Cambridge: MIT Press, 2013.

PRICE, S. A. Understanding Contemporary Cryptography and its Wider Impact upon the General Law. **International Review of Law, Computers & Technology**, v. 13, n. 2, p. 95-123. 1999.

ROGAWAY, P. The moral character of cryptographic work. **Cryptology ePrint Archive**, p. 2-48. 2015.

TANCZER, L.; McCONVILLE, R.; MAYNARD, P. Censorship and Surveillance in the Digital Age: The Technological Challenges for Academics. **Journal of Global Security Studies**, v. 1, n. 4, p. 346-355. 2016.