SH SCIENTIARUM HISTORIA
REVISTA DE HISTÓRIA DAS CIÊNCIAS E DAS TÉCNICAS E EPISTEMOLOGIA
ISSN 2675-6404

Ética: qual o cenário de pesquisa no Simpósio Brasileiro SBSeg?

Ethics: what is the research scenario in the Brazilian Symposium SBSeg?

Luiz Paulo CARVALHO
Instituto de Computação
Universidade Federal do Rio de Janeiro
luiz.paulo.carvalho@ppgi.ufrj.br

Flávia Maria SANTORO
Departamento de Informática e Ciência da Computação
Universidade do Estado do Rio de Janeiro
flavia@ime.uerj.br

Lisandro Zambenedetti GRANVILLE
Instituto de Informática
Universidade Federal do Rio Grande do Sul
granville@inf.ufrgs.br

Abstract. *Ethics and Information and Computer Systems Security go hand in hand. Security is related to freedom from risk or the threat of change for the worse and is directly associated with moral values and evaluation. In Brazil, the largest and most important event related to this topic is the Brazilian Symposium on Information and Computational Systems Security (SBSeg) of the Brazilian Computer Society. This paper aims to investigate the occurrence of ethical aspects in SBSeg's. How does ethics explicitly permeate research published in SBSeg between 2001 and 2021? By responding to this research question, the results indicate that the respective Brazilian community is far from dealing with ethical aspects in its scientific communications. We discuss this result, bringing analyzes and interpretations containing concerns, and future work.*

Keywords: *Computer Ethics. Information and Computer Systems Security. Metascience. Systematic Literature Review. Ethics Committee and Informed Consent.*

Resumo. Ética e Segurança da Informação e de Sistemas Computacionais andam de mãos dadas. A segurança está relacionada à ausência de risco ou ameaça de mudança para pior e está diretamente associada a valores morais e avaliação. No Brasil, o maior e mais importante evento relacionado ao tema é o Simpósio Brasileiro de Segurança da Informação e Sistemas Computacionais (SBSeg) da Sociedade Brasileira de Computação. Este trabalho tem como objetivo investigar a ocorrência de aspectos éticos na SBSeg. Como a ética permeia explicitamente as pesquisas publicadas na SBSeg entre 2001 e 2021? Ao responder a essa questão de pesquisa, os resultados indicam que a respectiva comunidade brasileira está longe de tratar de aspectos éticos em suas comunicações científicas. Discutimos esse resultado, trazendo análises e interpretações contendo inquietações e trabalhos futuros.

Palavras-chave: Ética Computacional. Segurança de Sistemas Computacionais e Informação. Metaciência. Revisão Sistemática da Literatura. Comitê de Ética e Consentimento Informado.

Recebido: 14/03/2023 Aceito: 14/12/20ZZ Publicado: 20/12/2023

DOI:10.51919/revista_sh.v1i0.411

1. Introduction

Ethics and Information and Computer Systems Security (ICSS) go hand in hand. This relationship is trivial to understand. Cambridge dictionary defines security as *freedom from risk, the threat of change for the worse + freedom from danger and safety* [1]. To *something* be freed from risk, the threat of worsening, or danger, there must be an associated moral value and evaluation.

Until the Cambridge Analytica scandal (SPINELLO, 2020), the perception of overall risk in handling personal data, particularly non-sensitive data, was minimal. Most of the population, laypeople, did not realize those data combinations such as, hypothetically, *likes Hello Kitty page + watches Friends* could determine the probability of being a specific political propaganda target and disseminate exclusive content for this target audience (SUMPTER, 2018). Without this target audience or other users knowing, without any content and practice mediation.

As morally catastrophic events, scandals serve as dialogic fuel between technology(ies) and society(ies) (MOOR, 2005). Consequently, several countries or blocks of countries currently have or plan to have laws related to handling personal data, such as the Brazilian General Data Protection Law (*Lei Geral de Proteção de Dados* – LGPD) (BRASIL, 2018). Several other countries, in turn, forward legal norms related to the subject, morally acting on this subject.

[1] Available at: https://dictionary.cambridge.org/dictionary/english/security [Accessed 15 Nov. 2023]

ICSS is primarily ethics-dependent. To be something positive to be preserved or secured, there must be something negative related. In this sense, this something and its valuation as positive or negative are related to morality, which in turn depends on cultural, historical, and social elements (BRASIL, 2016; VASQUEZ, 2018). The same applies to research, which is why academic-scientists conceived and consolidated research ethics and consolidated, fostered by the horrors of the so-called scientific experiments that took place in World War II (BLUNDELL, 2021). It also includes security related to research ethics involving computational solutions, e.g., when the University of Minnesota carried out a scientific experiment exploring sociotechnical vulnerabilities related to Linux and its community, defined by many as an *unethical* scientific practice regarding security (CHIN, 2021).

In Brazil, the largest ICSS and cryptography event is the Brazilian Symposium on Information Security and Computational Systems (*Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais* – SBSeg) of the Brazilian Computer Society (*Sociedade Brasileira de Computação* – SBC). SBSeg range from Computing Ethics (CE) classics (e.g., such as privacy, Intellectual Property (IP), and improper access) to almost purely technical issues (e.g., secure hardware or security of specific systems). Both the central concept, ICSS, and many of the related topics addressed by SBSeg are ubiquitous elements in the CE literature, and we investigate whether this is a symmetrical relationship. We seek to answer the research question: *how does ethics explicitly permeate research published in SBSeg between 2001 and 2021?* Indirectly, does the Brazilian ICSS community value computational ethics as much and in the same way that computational ethics means and values ICSS?

We also investigate secondary elements related to the research. We cover the Ethics Committee (EC) and Informed Consent (IC) topics, which are essential for research ethics (RECKER, 2021; SALGANIK,2017). These two elements are strictly security-related, designed to safeguard, anticipate, or prevent any potential harm, risk, or danger that research may bring, both for the participant and the researcher responsible for the moral values of their scientific practice.

EC and IC are topics mostly present in knowledge artifacts from the Health domain, e.g., Medicine. Other knowledge domains communities or entities present knowledge artifacts covering EC and IC, primarily or secondarily, e.g., Education (ANPED, 2021). Currently, structured and formalized knowledge agency about EC or IC is rare to find in Computing as a whole, mainly in an official and formal way by their communities or entities, such as Health or Education.

To answer the research question, we followed the scientific rigor of a Systematic Literature Review (SLR), according to the protocol proposed by Kitchenham and Charters (2007), detailed in Section 3. The results indicate that the relationship of interest in both topics is not mutual. The Brazilian ICSS community is far from discussing or dealing with ethical aspects in its scientific communications. We discuss the results, bringing analyzes and interpretations containing further questions and concerns, even as potential future work.

To the best of our knowledge, this present work is unprecedented in the Brazilian context, indicating its innovative character. At the same time, we intend to mature the meta-research (IOANNIDIS, 2018) debate related to Brazilian computing and ICSS, reinforced by the event's longevity, community strength, and contemporary domain relevance.

This work is structured as follows. In Section 2, we present the concepts that guide this research and related works. In Section 3, the methodology; Section 4, the associated results; and discussions in Section 5. Section 6 concludes this paper.

2. Ethical foundations and related works

Despite the potential for the intersections between ethics and ICSS to yield content worthy of an entire book, we will strive for conciseness and brevity. Simply, ethics, or Moral Philosophy, analyzes the question of *what to do?* (FERRAZ, 2014). The object of the study of ethics is morality, which, in turn, dialogues with values such as good, bad, right, wrong, and fair (BLUNDELL, 2021). Ethics deals with practices, such as customs, traditions, and habits. An act must be rational, free, conscious, and accountable to be ethical (VASQUEZ, 2018).

Being ethical is not the same as *being good*. Morality governs *goodness*, and morality is a context-dependent ideology (VASQUEZ, 2018). Value evaluation is inherent to morality, while ethics deals with higher-level dilemmas and reflections. In this sense, a cybercriminal who acts rationally, knowingly, freely, and accountable, is considered an ethical entity, although deliberately immoral. Hall (2014) defines CE as:

> Computing ethics is the interdisciplinary and collaborative efforts of scholars and professionals to methodically study and practically affect the contributions and costs of computing artifacts in global society. (HALL, 2014, p. 28)

ICSS collective importance of responsibility is unique. Responsibility and accountability are necessary for ethical decision-making (VASQUEZ, 2018), and the ICSS is the most critical from the CE's perspective. Balancing genuine ignorance and risks with potential harm is crucial.

ICSS presents a potential active or passive risk. And this reinforces the ethical relevance of the practical-utility requirement qualities. In this sense, two cases are possible. There is a passive risk when failures happen without the adversarial intent of the counterpart. For example, a curious enthusiast digs through the code and finds a vulnerability. The system developer unknowingly generated a glitch, and some onlookers stumbled upon it.

There is an active risk considering the adversarial dynamic. Adversaries actively provoke or attack the system, requirements, and developers. Active risk has been native to ICSS and the subject of CE research for many years (WECKERT, 2007; JOHNSON, 2008; REYNOLDS, 2019).

Passive risk is relatively simple, so we linger on active risk. Not every adversary [2] acts in bad faith (MANJIKIAN, 2017; MASIERO, 2013). Suppose the case in which a student took institutional classes on how to hack email. The student uses a technique learned by the respective institution only to invade an email box. In good faith, the password may be very simple or obvious, and the student notifies the target to strengthen it later. We could also debate the morality of this improper access. What is the harm caused by simple access? Should the principle of privacy and preservation precede consequences? If the target's password remains of poor quality, is a greater risk of a harmful future event? If the student had improperly accessed and not been notified about this action, would it be a dilemma or a moral fault in the same way?

Several motivations lead to a scenario with active ICSS risk. For example, challenge your own technical capabilities of invasion, fun, distraction, teasing the opposing party, and overcoming your expertise, among others (MASIERO, 2013). Not all adversarial interactions have negative motivations, intentions, justifications, or expectations, excluding practices in controlled environments, e.g., the public safety tests for Brazilian electronic voting. Other adversarial interactions have hidden or implicit intentions, such as attackers who exploit vulnerabilities, purposely letting themselves be caught, waiting for job opportunities to precisely address these vulnerabilities. Although good faith is dubious, bad faith is absent.

We sought to expose ICSS situations and opportunities for dilemmas or reflections, e.g., a 13-year-old boy who breaks into a critical hospital system and leaves an innocuous trail for fun is categorically different from a 25-year-old man who knocks out a hospital's electrical grid, causing pain, discomfort, and potentially death to many people. Some cases present objective bad faith, i.e., intent to cause harm, pain, or loss. They should be held accountable and possibly punished. The punishment will differ based on other elements, such as justification or intention.

Following the research protocol (KITCHENHAM & CHARTERS, 2007), the first step is to probe for competing or similar works. If they exist, we could complement or criticize them. As previously mentioned, we did not find any national or international SLRs competing with this one. Searches on the *Portal de Periódicos CAPES* and Google Scholar present no output of competing or similar works, considering the search string *ETHICS AND INFORMATION AND COMPUTER AND SYSTEM AND SECURITY*.

We found an SLR on CE, covering several of the most cited and discussed topics in related CE work. Stahl *et al.* (2016) cover 599 documents and extract knowledge from them using Grounded Theory. On the most frequently encountered issues, privacy is the first place, with more than twice as many occurrences concerning the second, also figuring security, harm, misuse, deception, and online piracy. The concept of responsibility is one of the most frequent

[2] We categorize this entity as "adversary" and not by culturally perceived negative terms (as criminal or hacker) until the value judgment of the moral act is defined. The moral quality of this act is undefined.

topics in ethical theories. The technological domains are varied, for example, computer surveillance, robots, e-Health, and computer games.

We turn to the CE literature, aiming to stress the relationship between CE knowledge and SBSeg publications. We reviewed several CE books analyzing the current ICSS topics. From the most traditional and cited books in the area to less prestigious ones. We prioritize works published in the 21st century. As an expected result, all of them deal with ICSS-related topics. As the only Brazilian book dedicated to CE found, Masiero (2013) covers unauthorized or improper access, privacy, copyright, and security of critical systems.

We list CE books widely found on the internet and in standard repositories. Blundell (2021), privacy, surveillance, research ethics. Johnson (2008), privacy, IP surveillance, online crime, hacking. Reynolds (2019), cyberattacks and cybersecurity, privacy, IP. Tavani (2008), privacy, anonymity, hacking, hacktivism, counter-hacking, cyber conflict, IP. Kizza (2016), anonymity, security, privacy, IP, and computer crimes. Barger (2008), theft, privacy. Baase & Henry (2017), privacy, IP, crime, and security – devotes an entire chapter to *errors, failures, and risks*. Here we classify them as passive risks, indicating how they can be associated with a security problem or cases culminating in one. Hoven (2008), privacy, research ethics. Weckert (2007), privacy, IP, surveillance, hacking; Spinello (2020), privacy, IP, security, cybercrime, hacking. Specifically, Manjikian (2017) is entitled *Cybersecurity Ethics, An Introduction*, which covers privacy, surveillance, IP, and cyberwarfare. Weckert (2007), Tavani (2008), and Hoven (2008) feature chapters, parts, or sections dedicated explicitly to Responsibility.

After analyzing more than ten books, from the most prestigious and cited to the least, we realized that ICSS is ubiquitous in the broad CE literature. We perform a superficial and brief scan for explicit and objective occurrences. Privacy follows this behavior as a significant interest.

Even though not all have sections, parts, or chapters dedicated to hacking, the terms hack, or hacker is present in all books. Even outside the main scope of this work, it surprises us how these terms, respectively the people categorized by them, are negatively valued (KIZZA, 2016; BAASE & HENRY, 2017; SPINELLO, 2020). When dealing with moral judgment and value, it is plausible that cultural aspects related to the popularly well-established definition of hacking prevail [3]. On an ethical level, especially in academic-scientific books. It even realistically disregards the entire community and the idea of ethical hacking (MANJIKIAN, 2017).

3. Research methodology and method

We follow the same SLR research protocol, based on Kitchenham and Charters (2007) and from previous works (CARVALHO *et al.*, 2021; CARVALHO *et al.*, 2022).

[3] Available at: https://www.merriam-webster.com/dictionary/hacker [Accessed 15 Nov. 2023]

In summary, we obtain all openly available publications from SBSeg between 2001 and 2021, i.e., we analyze 21 years of SBSeg proceedings. Then we search for the terms through a string search, year by year. Wide screening is the name of the initial phase. After extracting the terms and highlighting the associated papers, another researcher reviews this extraction to prevent bias or possible errors. This step is objective, based on the extraction terms.

The narrow screening follows. We analyze each paper and its ethical aspects' relevance, i.e., the paper deals with explicit ethical aspects with relevance, depth, and significance. We send the extracted papers from narrow screening for qualitative synthesis, viable due to the ethical aspects' quality alignment.

Finally, we answer the research sub-questions from the main question in the qualitative synthesis, extracting and generating information and knowledge. We distribute the extraction among the researchers. After the data and information extraction, other independent researchers reviewed it again to present bias or possible errors. The final result is the concatenated and processed information, generating the SBSeg ethical panorama.

That was the *planned* method, following the research protocol strictly. It turns out we did not get past the wide screening. The number of occurrences of the search string terms in the wide screening was negligible, with only 12 (≈0.015%) occurrences among all 793 papers. In comparison, the wide screening on Human-Computer Interaction (IHC-BR) (CARVALHO *et al.*, 2022) resulted in 218 (≈28%); in Games (SBGames) (CARVALHO *et al.*, 2021) resulted in 322 (≈18%). After the narrow screening, we did not even get close consensual interpretive assessment in the qualitative synthesis (KITCHENHAM & CHARTERS, 2007).

In this case, we will detail the procedure until the conclusion of the wide screening. Then we will forward the discussions. Between the years 2001 and 2011, we analyze only main track papers. We download 2001 to 2011 papers and 2018 to 2021 papers from the website of the Special Commission (CESeg) and in the SBC Open Library (SOL). From 2012 to 2017, they publish the proceedings as a single file. In the 793 papers, we searched for the search strings, also considering the inclusion and exclusion criteria.

The search strings: *ETHIC AND ETIC AND ÉTIC AND MORAL AND MORAIS AND CONSENT*. Wide screening inclusion criteria: mention ethical-based terms directly associated with the search string + mention informed consent or ethical committee + ethical-based terms in body text. Wide screening exclusion criteria: does not mention ethical-based terms directly associated with the search string + does not mention informed consent or ethical committee + ethical-based terms occur only in references, abstract, direct citations/quotes, title(s), or keywords. Narrow screening inclusion criteria: mention ethical-based terms in-depth, and broadly considered + ethical aspects adhere to the definitions considered in this paper. Narrow screening exclusion criteria: mention ethical-based terms superficially + ethical aspects do not adhere to the definitions considered in this paper.

After applying the criteria, the wide screening resulted in 12 results. To mitigate threats to validity, promote auditability and reproducibility, and Open Science, the wide screening result and deepening is available in Table 1. In narrow screening, none of them was considered eligible by consensus, we present the reasonings in Table 1. We omitted the research sub-questions by conciseness. In this sense, we will briefly discuss the wide screening results.

Research ethics standards vary from country to country. Wangham et al. (2018) reiterate that scientific research using patient data should be submitted and appreciated by EC. They could have cited the official resolution (466/2012) (BRASIL, 2012) of the National Health Council, but instead, they referenced an international conference paper.

Leite & Salles (2019) forward a meta-research moral qualification. For alleged ethical reasons, the research practice only creates fake Facebook profiles without using malware to acquire existing accounts to integrate the social botnet. This intention seems morally acceptable because it avoids harming other accounts of legitimate users. However, Facebook's community policies do not allow the creation and maintenance of fake accounts on the platform [4], i.e., there is a regulatory violation. So, are the benefits, contributions, and research findings worth violating the platform's moral norms? Should the researchers have sought Facebook's permission sooner? Is the moral quality of the research compromised because it violates the platform contract?

Table 1. Wide screening selected papers

Term	Year	Title	Excerpt*
etica	2001	SCOM: SCAN DE PORTAS DE COMUNICAÇÃO REMOTAS (Martins and Monteiro, 2001)	"Atualmente não há como falar em sites Internet sem mencionarmos segurança, mas, o questionamento sobre o grau de segurança que os desenvolvedores podem alcançar na construção de suas aplicações, geralmente, inexiste devido a ética de alguns profissionais que estudam constantemente para criar técnicas de burlar os sistemas para fins ilícitos."
morais	2002	Resposta a Incidentes para Ambientes Corporativos Baseados em Windows (Oliveira et al., 2002)	"A complexidade envolvida no trato com incidentes de segurança somadas ao nervosismo causado pela iminência de prejuízos morais e financeiros, justificam a criação de um TR, que por sua vez, estará encarregado da definição dos procedimentos a serem adotados no caso de uma emergência. "
etica/etico	2010	AnonV: uma arquitetura para verificac¸ao do grau de ˜ anonimizac¸ao em coletas de tr ˜ afego de rede (de Melo e Guedes, 2010)	"O ` administrador pode ate ter interesse no tipo de resultado esperado, mas s ´ o pode fornecer ´ os dados se tiver garantias de que a privacidade dos seus usuarios n ´ ao ser ˜ a violada em ´ relac¸ao ao que exige a lei e a ˜ etica, o que poderia implicar em um an ´ alise detalhada da ´ferramenta oferecida." + "Tambem s ´ ao encontrados alguns ˜ artigos que analisam a etica e os problemas jur ´ ´ıdicos que o compartilhamento de dados pode gerar [...]"
moral	2010	Produção de Provas Digitais a partir de Rastreamento em	"Em paralelo, no estudo de [...], palavras que caracterizam assédio moral no ambiente de trabalho foram coletadas de diversas

[4] Available at: https://transparency.fb.com/policies/community-standards/account-integrity-and-authentic-identity/ [Accessed 15 Nov. 2023]

		Relacionamentos por e-mails (Mallmann et al., 2010)	maneiras, passando inclusive por pré-processamento."
etica	2012	Analise de M ´ etodos de Aprendizagem de M ´ aquina para ´ Detecc¸ao Autom ˜ atica de ´ Spam Hosts (Silva et al., 2012)	"Existem diversas estrat´egias ´eticas de SEO, por´em como afirma [...], para aprender as mais bem sucedidas, ´e preciso muito tempo e dedicac¸˜ao."
etica	2012	Um Modelo de Seguranc¸a e Privacidade para Redes Sociais Moveis Aplicadas ´ a` Area da Sa ´ ude (Gonçalves et al., 2012)	"A seguir, foram identificados os requisitos espec ´ ´ıficos de seguranc¸a e privacidade, onde verificou-se que os mesmos deveriam seguir um conjunto de restric¸oes legais e ˜ eticas definidas pelo Conselho Nacional de Sa ´ ude ´ 2 e um conjunto de padroes e requisitos presentes no Manual de Certificac¸ ˜ ao para Sistemas de ˜ Registro Eletronico em Sa ˆ ude [...], editado pela Sociedade Brasileira ´ de Informatica na Sa ´ ude (SBIS). "
moral	2013	O estado da arte da legislação brasileira sobre a criminalidade cibernética (Valverde e Silva, 2013)	"A tecnologia da informação possibilita, nos dias atuais, a perpetração de dano ou de perigo de dano contra o patrimônio moral e material dos indivíduos e, com frequência, da própria coletividade, que, pela sua gravidade teria de ser objeto da incidência pena"
ética	2018	O Futuro da Gestão de Identidades Digitais (Wangham et al., 2018)	"Qualquer pesquisa científica que envolva uso de dados dos pacientes deve ser previamente autorizada pelos comitês de ética em pesquisa médica, que prezam sempre a privacidade dos dados, o anonimato e o bem-estar dos pacientes [...]. "
ethic	2018	Privacy-preserving recommendations for Online Social Networks using Trusted Execution Environments (Rossi et al., 2018)	"However, by using these services, users leave behind a large trail of data that may be accessed and used in unethical practices [...]."
moral	2018	Avaliac¸ao de mecanismos de consenso para blockchains em ˜ busca de nova estrategia mais eficiente e segura (Aliaga et al., 2018)	As caracter´ısticas que dificultam fraudes sao muito variadas. Entre as mais interessantes ˜ esta a trag ´ edia dos comuns, um princ ´ ´ıpio moral que governa o mecanismo PoA, o qual tenta manter o bem comum entre os usuarios: se algum usu ´ ario age mal, prejudica todos, ´ inclusive a si mesmo.
etica	2019	Design e implementac¸ao de uma arquitetura conceitual para a ˜ criac¸ao de ˜ social botnet em redes sociais (Leite e Salles, 2019)	"Entao, por quest ˜ oes ˜ eticas, a ´ social botnet contru´ıda nesta pesquisa nao contempla ativi- ˜ dades maliciosas para aquisic¸ao de contas, como disseminac¸ ˜ ao de ˜ malware. Portanto, a abordagem utilizada neste artigo e a criac¸ ´ ao de perfis falsos." + "´ alido ressaltar que embora o uso ´ de malware facilitasse o processo de aquisic¸ao de contas para a ˜ social botnet e a sua infiltrac¸ao, n ˜ ao foi usada tal abordagem como premissa por quest ˜ oes ˜ eticas."
ética/ético	2021	WebGoat Plus: Uma Extensão da Ferramenta WebGoat para o Ensino de	3 occurrences of ethics, only in related works

		Vulnerabilidades de Segurança (Bizon e Justino, 2021)	

* Excerpts of texts extracted here are copied and pasted exactly as in their original documents. Character encoding issues were maintained, we discuss their occurrence at Section 5.

Bizon & Justino (2021) was the closest to adherence, but they restricted the ethical consideration of hacking teaching and ethics training to related works.

Valverde & Silva (2013) brings up a rare topic in SBSeg, mainly due to its sociotechnical scope, cyberbullying. Kizza (2016) analyzes this topic from the CE perspective. Morality is shallow, without depth, indicating that information technology makes it possible to perpetrate damage to individuals' moral and material patrimony. Instead of embarking on ethics, they conduct the study based on laws and norms. It is worth remembering that ethics and laws are not synonymous (Barger, 2008; Vasquez, 2018). Acting blindly just following the law(s) is not a necessary and sufficient condition for ethical qualification.

Observing Table 1, in addition to the works mentioned above, the occurrences in the excerpts are explicitly superficial and brief, the only ones found in them. With just one occurrence, it is difficult to go into depth or detail the ethical or moral aspect(s).

4. Discussion

Considering the result of the SLR search and extraction procedure, we seek to extend knowledge by discussing related subjects and secondary analyses. At this point, we can already answer the question that guides this research. Explicit ethical aspects are absent from the SBSeg, i.e., they permeate less than 0.1% of the publications in more than twenty years of the symposium.

Considering the **asymmetry of interest between areas**, we can see the scarcity of ethical aspects in SBSeg publications. As a complement, we searched at the references, excluded in the screening stages, on the occurrences of ethics or morals to perceive if they occur referencing CE works despite explicit occurrences not occurring in the body text. We notice an asymmetry of interest between both areas. While CE resorts abundantly to ICSS in its analyses, the opposite does not happen. It indicates the absence of formal dialogue or interest in knowledge generated in these themes through scientific communications.

Considering the covered range of SBSeg, between 2001 and 2021 we did not find occurrences of topics of interest mentioning ethics or morals, either explicitly or through related terms. Through a simple intertextual analysis, it connotes a lack of interest related to these terms, whether due to negligence or ignorance, related to these terms and their associations with ICSS.

What about research ethics? One of the most alarming results was the absence of any occurrence of the term *CONSENT*, which indicates the IC of research involving human participation. Regarding research ethics, consent is one of the primordial points, considered a general rule and an exception only in rare and very specific cases (SALGANIK, 2017). The

institutional moral norms of research ethics make it mandatory to obtain and register free and informed consent from research participants (BRASIL, 2012; BRASIL:2016).

Research involving humans must be submitted and appreciated by an EC (BRASIL, 2012; BRASIL, 2016). We went through the last three editions of SBSeg (2019, 2020, 2021) using the search term participant, resulting in a few occurrences. Despite human participation in these studies, there is no mention of IC. If there was a concrete involvement of IC, scientific communication disregards a deficiency in terms of the completeness of procedural research information. By association, the occurrence of EC was also null.

Valverde & Silva (2013) involves cyberbullying, Bizon & Justino (2021) are brief and limited about hacking instruction in an educational environment, and many others from the 793 papers expose potential that overflows the strictly technical or technological boundaries. There is a potential for research to go beyond the technical aspect, covering human or procedural phenomena.

We stress the *target* of ICSS research, reinforcing the need for a sociotechnical vision. Research, especially pragmatic research, aims to solve a problem associated with a phenomenon where the ultimate benefit, advantage, or improvement is people-oriented. People are (or should be) the target audience of any academic-scientific research (RECKER, 2021; VARSAVSKY, 1973), i.e., when developing a solution or computational artifact, the goal should be people-oriented, even if directly associated with another solution or computational artifact.

When proposing an improvement in a cryptography system, the focus is on cryptography systems, but the final link in this chain is society, i.e., people. Science, void of social, cultural, or historical intertwining and carried out only for scientific benefit, is scientism (VARSAVSKY, 1973), alienated from reality and concrete societal values.

The *technical and pragmatic* prevalence is dreary. Computational systems and artifacts need improvements, and the dialogic interaction with reality demands new ones as well. Technical research and development are essential for computing and its technologies. Analyzing SBSeg publications, there is a predominance of technical or pragmatic academic-scientific research. Culminating is a challenge to ethical aspects, as related to social, cultural, and historical data.

SBSeg is the largest Brazilian ICSS symposium and the largest gathering space for this theme, with knowledge epistemology intrinsically related to ethics and morals. The technical or pragmatic predominance and bias are just a scientific, cultural, and political character of the SBSeg researcher's scientific practices. To say this is a problem would be to value this reality negatively, and we would leave the ethical scope. We expected a greater occurrence of ethical aspects and indicated that there is space to cover them, e.g., scrutinizing the CE literature.

At first, it seems that **SBSeg would be the ideal place for this communication**. The rejection in the SBSeg 2022 announces: *It is expected, for the SBSEG, that the article proposals are related to technical issues*. Paired with: *Maybe the explicit treatment of ethics is not required for a large*

number of SBSeg papers, and ethical aspects of security technologies are a multidisciplinary subject more adequate for another type of conference.

Still, we were unable to find other Brazilian ICSS formal academic-scientific communication. Considering the epistemology of ICSS technologies, this indication could signify the funeral of this research. Despite this, after exposing the reasoning of the multidisciplinary epistemological intertwining, we feel obliged to formalize, as recommended to us, in an appropriate place.

If our primary intention is to criticize the same phenomenon that led to the rejection in the proper epistemologically adequate community, here we riot. Ethical aspects are beyond human sciences, technical issues, multidisciplinary, and this is philosophically fundamental.

5. Final remarks

The negligible occurrence of ethical aspects in mere (≈0.013%) of all 793 papers in 21 years of SBSeg, is not indicative that the ICSS community is unethical, immoral, or ignorant of the topic. Rather, it clearly and objectively indicates that explicit ethical aspects are absent. Ignorance, negligence, or disregard for the sociotechnical character causes part of this absence without reflecting the entire community or the entire SBSeg. What is perceived is, in fact, a potential to plant and cultivate ethics or morals.

As a contribution, in Section 3, we indicate CE books, and respective topics related to ICSS, for appreciation and possible dialogue by those interested in this intersection. Or, even more, enriching their research with ethical aspects.

Although technical or technological aspects predominate in ICSS academic-scientific spaces, we noticed some spaces of epistemological insurgencies in ethical or moral aspects. As concrete examples, the 1st International Workshop on Ethics in Computer Security[5] and the Workshop on Transparency, Accountability and User Control for a Responsible Internet[6]. Some call for papers presents terms directly related to Ethics, such as Trust, Privacy, Reliability.

There is an intrinsic moral feature in ICSS: the *security* intent. It would be more appropriate and better if the search for security and correlates had an ethical appreciation, enriching the proposal at a philosophical level. From an ethical point of view, the mere intentional dedication to free society of risks, danger, or threat of change for the worse is a collective moral advancement (VASQUEZ, 2018). Despite that, the rationality of the moral act is beyond the individual or group intentional altruism of the researcher(s), and even if there is a positive intention, the other moral elements may lack quality. For example, motivation, justification, or possible consequences - elementary components of the moral act - may be compromised. And ethics assists in this self-inspection.

[5] Available at: https://ethics-workshop.github.io/2022/ [Accessed 15 Nov. 2023]
[6] Available at: https://taurin2023.responsible-internet.org/ [Accessed 15 Nov. 2023]

We hope these findings bring reflection and maturity to consider the state of Brazilian ICSS's ethical aspects. Cover other ICSS communications is a proposal for future work.

Funding

This study was funded by the Coordination for the Improvement of Higher Education Personnel - Brazil (CAPES) - Financial Code 001.

References

ALIAGA, Yoshitomi Eduardo Maehara; LEAL, Victor Cerqueira; LUCENA, Antônio Unias de; HENRIQUES, Marco Aurélio Amaral. Avaliação de mecanismos de consenso para blockchains em busca de nova estratégia mais eficiente e segura. In: **SIMPÓSIO BRASILEIRO DE SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS (SBSEG), 18., 2018, Natal. Anais [...]**. Porto Alegre: Sociedade Brasileira de Computação, 2018. p. 33 - 40.

ANPED, C. de Ética em P. Ética e pesquisa em educação: subsídios - volume 1. **Boletim Técnico do PPEC**, Campinas, SP, v. 6, n. 00, 2021. Disponível em: https://econtents.bc.unicamp.br/boletins/index.php/ppec/article/view/9431. Acesso em: 15 nov. 2023.

BAASE, S; Henry, T. M. **Gift of Fire, A: Social, Legal, and Ethical Issues for Computing Technology**. 5th ed. New York: Pearson, 2017.

BARGER, R. **Computer Ethics: A Case-Based Approach**. Cambridge: Cambridge Univ. Press, 2008.

BIZON, A.; Justino, G. Webgoat plus: Uma extensão da ferramenta webgoat. *In*: **Anais Estendidos do XXI SBSeg**, p. 138–150. Porto Alegre: SBC, 2021.

CARVALHO, L. P. *et al.* Ética: Qual o Panorama de Pesquisa no Simpósio Brasileiro SBGames? *In*: **Anais do XX SBGames**. Porto Alegre, SBC, 2021. ISSN: 2179-2259.

CARVALHO, L. P. *et al.* A meta-scientific broad panorama of ethical aspects in the Brazilian IHC. **Journal on Interactive Systems**. Porto Alegre, v. 13, n. 1, p. 105 – 126, 2022.

BLUNDELL, B. G. **Ethics in Computing, Science, and Engineering: A Student's Guide to Doing Things Right**. New York: Springer, 2021

BRASIL. **RESOLUÇÃO Nº 466, DE 12 DE DEZEMBRO DE 2012**. Ministério da Saúde, Conselho Nacional de Saúde, [2012]. Available at: https://cutt.ly/mmS8Eua. Accessed: 15 Feb. 2023.

BRASIL. **RESOLUÇÃO Nº 510, DE 07 DE ABRIL DE 2016**. Ministério da Saúde, Conselho Nacional de Saúde, [2016]. Available at: https://cutt.ly/yjSF2Lm. Accessed: 15 Feb. 2023.

BRASIL. **LEI Nº 13.709, DE 14 DE AGOSTO DE 2018**. Brasília, DF: Presidência da República, [2018]. https://4658.short.gy/thJx59. Accessed: 15 Feb. 2023.

CHIN, M. **HOW A UNIVERSITY GOT ITSELF BANNED FROM THE LINUX KERNEL** [2021]. https://4658.short.gy/TzjXZU. Accessed: 15 Feb. 2023.

COSTA, T.; Sergio, M.; Marin, R. Entendimento dos controles e possíveis conflitos de privacidade nas redes sociais online. *In*: **Anais Estendidos do XIX SBSeg**, p. 57 – 60. Porto Alegre: SBC, 2019.

FERRAZ, C. A. **Ética Elementos Básicos**. Pelotas: NEPFIL, 2014.

GONÇALVES, Jesseildo; TELES, Ariel; SILVA, Francisco José. Um Modelo de Segurança e Privacidade para Redes Sociais Móveis Aplicadas à Área da Saúde. In: **SIMPÓSIO BRASILEIRO DE SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS (SBSEG), 12., 2012, Curitiba. Anais [...]**. Porto Alegre: Sociedade Brasileira de Computação, 2012. p. 338-344. DOI: https://doi.org/10.5753/sbseg.2012.20559.

HIMMA, K. E.; Tavani, H. T. **The handbook of information and computer ethics**. Hoboken: John Wiley & Sons, 2008.

IOANNIDIS, J. P. A. Meta-research: Why research on research matters. **PLoS Biol**. New York, v. 16, n. 3, 2018.

JOHNSON, D. G. **Computer Ethics**. 4th ed. New York: Pearson, 2008.

JÚNIOR, C. *et al.* Capture the flag: Método de aprendizado para a disciplina de forense computacional em uma universidade pública. *In*: **Anais Estendidos do XIX SBSeg**, p. 155–158. Porto Alegre: SBC, 2019.

KITCHENHAM, B.; Charters, S. **Guidelines for performing systematic literature reviews in software engineering**. Technical Report EBSE 2007-001. Keele Univ. and Univ. of Durham, 2007.

KIZZA, J. M. **Ethics in Computing A Concise Module**. New York: Springer Cham, 2016.

LEITE, V.; Salles, R. Design e implementação de uma arquitetura conceitual para a criação de social botnet em redes sociais. *In*: **Anais do XIX SBSeg**, p. 337 – 350. Porto Alegre, SBC, 2019.

MANJIKIAN, M. **Cybersecurity Ethics: An Introduction**. New York: Routledge, 2017.

MALLMANN, Jackson; FREITAS, Cinthia O. A.; SANTIN, Altair Olivo. Produção de Provas Digitais a partir de Rastreamento em Relacionamentos por e-mails. In: **SIMPÓSIO BRASILEIRO DE SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS (SBSEG), 10., 2010, Fortaleza. Anais [...]**. Porto Alegre: Sociedade Brasileira de Computação, 2010. p. 283-296. DOI: https://doi.org/10.5753/sbseg.2010.20594.

MARTINS, Stéphany Moraes; MONTEIRO, Claudio de Castro. SCom: Scan de Portas de Comunicação Remotas. In: **SIMPÓSIO BRASILEIRO DE SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS (SBSEG), 1., 2001, Florianópolis. Anais [...]**. Porto Alegre: Sociedade Brasileira de Computação, 2001. p. 119-131. DOI: https://doi.org/10.5753/sbseg.2001.21293.

MASIERO, P. C. **Ética em Computação**. São Paulo: EDUSP, 2013.

MELO, Marco Aurélio Vilaça de; GUEDES, Dorgival. AnonV: uma arquitetura para verificação do grau de anonimização em coletas de tráfego de rede. In: **SIMPÓSIO BRASILEIRO DE SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS (SBSEG), 10., 2010, Fortaleza. Anais [...]**. Porto Alegre: Sociedade Brasileira de Computação, 2010. p. 367-380. DOI: https://doi.org/10.5753/sbseg.2010.20600.

MOOR, J. H. Why we need better ethics for emerging technologies. **Ethics Inf. Technol.** New York, v.7, p. 111 – 119, 2005.

MORAES, V.; Vilela, J. Uma avaliação do cenário de detecção e evasão do acesso root no android. *In*: **Anais do XXI SBSeg**, p. 57–70. Porto Alegre: SBC, 2021.

MOSCA, M. Cybersecurity in an era with quantum computers: Will we be ready? **IEEE Security Privacy**. New York, v. 16, n. 5, p. 38 – 41, 2018.

OLIVEIRA, Flávio de Souza; GUIMARÃES, Célio Cardoso; GEUS, Paulo Lício de. Resposta a Incidentes para Ambientes Corporativos Baseados em Windows. In: **SIMPÓSIO BRASILEIRO DE SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS (SBSEG), 2., 2002, Búzios. Anais [...]**. Porto Alegre: Sociedade Brasileira de Computação, 2002. p. 16-23. DOI: https://doi.org/10.5753/sbseg.2002.21259.

RAMOS, A. G. **A redução sociológica**. Rio de Janeiro: UFRJ, 1996.

RECKER, J. **Scientific research in information systems: a beginner's guide**. 2nd ed. New York: Springer-Verlag Berlin Heidelberg, 2021.

REYNOLDS, G. **Ethics in Information Technology**. 6th ed. Independence: CENGAGE, 2019.

ROSSI, Guilmour; GOMES-JR, Luiz; ROSA, Marcelo; FONSECA, Keiko. Privacy-preserving recommendations for Online Social Networks using Trusted Execution Environments. In: **SIMPÓSIO BRASILEIRO DE SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS (SBSEG), 18., 2018, Natal. Anais [...]**. Porto Alegre: Sociedade Brasileira de Computação, 2018. p. 41 - 48.

SALGANIK, M. **Bit by Bit Social Research in the Digital Age**. Princeton: Princeton Univ. Press, 2017.

SILVA, Renato Moraes; ALMEIDA, Tiago A.; YAMAKAMI, Akebo. Análise de Métodos de Aprendizagem de Máquina para Detecção Automática de Spam Hosts. In: **SIMPÓSIO BRASILEIRO DE SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS (SBSEG), 12., 2012, Curitiba. Anais [...]**. Porto Alegre: Sociedade Brasileira de Computação, 2012. p. 2-15. DOI: https://doi.org/10.5753/sbseg.2012.20532.

SPINELLO, R. A. **Cyberethics: Morality and Law in Cyberspace: Morality and Law in Cyberspace**. 7th ed. Burlington: Jones & Bartlett Publishers, 2020.

STAHL, B. C.; Timmermans, J.; Mittelstadt, B. D. The ethics of computing: A survey of the computing-oriented literature. **ACM Comp. Surv**. New York, v. 48, n. 4, 2016.

SUMPTER, D. **Outnumbered: From Facebook and Google to Fake News and Filter bubbles The Algorithms That Control Our Lives**. New York: Bloomsbury Sigma, 2018.

VALVERDE, D.; Silva, J. O estado da arte da legislação brasileira sobre a criminalidade cibernética. In: **Anais do XIII SBSeg**, p. 267 – 280. Porto Alegre, SBC, 2013.

VAN DEN HOVEN, J.; Weckert, J. **Information Technology and Moral Philosophy**. New York: Cambridge Univ. Press, 2008.

VARSAVSKY, O. **Ciencia, Política Y Cientificismo**. 4th ed. Buenos Aires: Centro Editor de America Latina, 1973.

VÁSQUEZ, A. S. **Ética**. 39th ed. São Paulo: Civilização Brasileira, 2018.

WANGHAM, Michelle Silva et al. O Futuro da Gestão de Identidades Digitais. In: **WORKSHOP DE GESTÃO DE IDENTIDADES DIGITAIS - SIMPÓSIO BRASILEIRO DE SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS (SBSEG), 18., 2018, Natal. Anais [...]**. Porto Alegre: Sociedade Brasileira de Computação, 2018. p. 146 - 166.

WECKERT, J. **Computer Ethics**. New York: Routledge, 2007.