(How) Can Directive (EU) 2019/1937 on whistleblowers be used to build up a security and safety culture in Institutions?

Margit Scholl
Business computing and administrative informatics
Faculty of Business, Computing, and Law Technical University of Applied Sciences
Wildau (TH Wildau)
Germany

ABSTRACT: *The process of comprehensive digitization and the ease with which many people can be duped are being exploited in criminal attacks. For this reason, there can be no question that a security culture needs to be established in institutions to raise awareness and ensure the commitment of employees. However, virtualization changes our understanding of ethics, and this affects institutions as well as individuals and society. Many institutions have established guidelines in an attempt to make professional ethics and moral conflicts the subject of collaborative reflection and action. But are these viable? This process is now supported by Directive (EU) 2019/1937, which covers the protection of people reporting breaches of EU law. As a common minimum standard, the directive seeks to provide a high level of protection for these individuals, who are popularly known as whistleblowers. The scope of the directive goes far beyond the concerns of an institutional security culture—nevertheless, it applies to this too. The paper sets out to start a proper debate on the digital turn, the building of a security culture, and the dilemmas involved in long lists of regulations, which are no guarantee of commitment. The information security culture in institutions depends on the awareness and expertise of management and employees and relies on continuous communication and ongoing discussions to ensure concrete progress. How can this be achieved? In the attempt to find an answer to this question through extensive literature research, the fundamental importance of the term "ethos" emerged. Since people can change their views and beliefs after identifying and reflecting on inconsistencies, it is also possible for this awareness to be trained through a process of active communication, the participatory exchange of ideas and experience, and interactive learning.*

Keywords: Directive (EU) 2019/1937, Protection of Whistleblowers, ISO 37002:2020-08, Safety and Security Culture, Information Security, Competence Development, Learning Processes, Ethos/Ethics/Morality

Received: 28 November 2020, Revised 7 February 2021, Accepted 20 February 2021

DOI: 10.6025/isej/2020/7/2/40-57

1. Introduction

As of December 17, 2021, companies with 250 or more employees will be obliged to introduce a whistleblower system as per Directive (EU) 2019/1937. For these companies, there are only a few months left to meet the extensive requirements, and many of them are wondering what the background to this is, how a whistleblower system can be implemented, and what they should be paying attention to. Illegal and unethical behavior is a serious problem for companies [1]. "As the Internet has evolved into a more social and communicative tool and venue, the ethical issues have shifted from purely data driven to more

human-centered" [2]. It is also very "human" in respect of the diverse technical and organizational tasks involved in information security (IS). Many studies show that individual awareness-raising and training measures in IS often do not have long-term success in ensuring that the security guidelines of an institution are observed and accepted. This has very different causes in individual cases. In general, achieving behavioral changes also poses a challenge, highlighting differences in the moral and ethical values held by the individual and their employer. Such conflicted situations can, for example, lead individuals to turn against their employer's confidentiality conditions. According to Schanz and Müller-Vorbrüggen [3], ethics seem to have become a rare commodity in the institutions of our society. Crucial questions in the age of comprehensive digitization are analogous to [3:1091]: Are people allowed to do anything they want? Who is responsible? How are responsibility, social awareness, and ethical values to be cultivated? Do the concepts that have recently been developed in companies—such as the Global Compact (voluntary commitment), Corporate Social Responsibility, Corporate Citizenship Projects, and Corporate Ethical Responsibility—correspond to an underlying set of values?

Increasingly, global digitization is a key driver in the dynamics of hybrid threats, since it exposes new potential vulnerabilities in the state, economy, and open society (see [4]). This year's report on IT security in Germany by the Federal Office for Security in Information Technology (BSI) makes it clear that the threat remains critical [4]. According to the report, there is a continuing tendency for cybercriminals to use malware for mass attacks against individuals, companies, and other institutions [4]. Individuals and institutions must be alert to the malicious programs that are used to steal identity data and leaks that allow the theft of customer data. In addition, critical weaknesses have been observed in software and hardware products [4]. Internal perpetrators and insider threats can also not be ruled out. One further aspect of human influence in the security area is inadvertent human error, which is largely overlooked, even though it can be assumed to be the main cause of numerous security breaches [5]. More research is needed here to understand the impact of human error. The increased amount of work being done in home offices as a result of the COVID-19 pandemic, coupled with a sudden surge in the use of unchecked digitization products, has opened up much greater scope for criminal activities and attacks. Many institutions have failed to build a sustainable security and safety culture that can cope with the increasing switch to digital work. It is important to understand that building a security culture in an institution is a continuous process. For example, an IT security culture describes how questions relating to IT security are dealt with and involves a complex learning process in which common goals, interests, norms, values, and behavioral patterns are developed [6]. This affects both the institution and the society as a whole. "Culture is primarily communication" [7]. This is why building an IS culture in an institution also involves a learning process and relies on the ongoing discussion of ethos, ethics, moral interpretations, and human error.

The word ethics comes from the Greek *ēthos* (ἦθος) and means custom, habit, or general attitude: thus, ethics is the doctrine of correct action and intention [3:1094]. Ethics is primarily a mental and not a material matter [3]. For example, in the context of international projects, it should be noted that morality is fundamentally defined according to the prevailing culture, and a project manager abroad must take into account that European normative morality does not necessarily seem logical to other cultures and may not comply with the perceptions of other cultures [3:1095]. Profitability and morality may also make contradictory demands [3]—they are usually at odds with one another. This can be a source of conflict for an individual because anyone who neglects profit endangers their own company, while those who disregard values and morals undermine the foundations of successful business. Ethics is also an important topic at universities: §64 (3) of the new version of the Higher Education Act in Germany, which came into force in 2014, requires the establishment of ethics committees; these deal with and make recommendations on questions relating to the possible use of research results for non-peaceful purposes and to research projects on humans and animals [8]. However, the increase in the number of ethics committees in German faculties was the result of individual, non-concerted efforts [9]. It is certainly not just in Germany that action is required to develop an interdisciplinary understanding of the principles governing research ethics—for further insights into this problem and the associated terminology, see Horne [10].

Every sane person has to justify their actions and answer for the consequences [3]. If a person has caused damage (and they are in their right mind), they are held responsible for it [3]. For example, the responsibility for the success of a project obliges the project manager to endeavor to achieve the goals that have been set, while at the same time observing the fundamental values of human dignity and the specific rules of conduct within the particular context. It is therefore appropriate that the German Society for Project Management e.V. (GPM) has also adopted a code of ethics for project managers [11]. According to this, project managers influence the quality of life of every single person in society in their professional practice and must align their actions and decisions with the basic values of responsibility, competence, and integrity [11]. It is not enough to say, "We obey all the laws," because, importantly, this statement is not geared to the future [12].

The German nonprofit organization Informatics Society e.V. (GI) has also established guidelines in an attempt to ensure "that matters of professional ethics or moral conflicts become the subject of collaborative reflection and action" [13]. Their guidelines are designed to offer a point of orientation not only to their members but generally to everyone involved in the design, manufacture, operation, or use of IT systems [13]. In line with its guidelines, the GI seeks to engage and educate the public in the discourse on the ethical and moral issues involved as a way to assess the impact of IT systems and to understand and take into account the rights, needs, and interests of those parties who are affected by them. "In a networked world, it is imperative that all potential courses of action be subject to interdisciplinary consideration regarding their foreseeable impact and potential consequences" [13]. But how can we foster the willingness of all actors to critically question and evaluate their individual and collective actions in public discourse and, if necessary, to recognize the limits of their own powers of discernment, as the GI demands? The idea of "ethos" points the way. However, this paper cannot yet delineate a comprehensive answer to this question, as this should be preceded by a general debate in society about this key term, which would go beyond the scope of this article. Nevertheless, in section 3, the author will offer a few suggestions as a reference and starting point for understanding ethos.

Tip-offs from employees and other stakeholders play an important role in the prevention and detection of violations of legal provisions or internal rules and values [1]. The purpose of Directive (EU) 2019/1937 on the protection of people who report breaches of Union law (issued on October 23, 2019) is "to enhance the enforcement of Union law and policies in specific areas by laying down common minimum standards providing for a high level of protection of persons reporting breaches of Union law" [14]. Those "reporting persons" are popularly known as whistleblowers. In the first recital clause of the EU directive, the conflict at the public level is described as the motivation for the adoption of this directive: by reporting violations of Union law that affect the public interest, "such persons act as 'whistleblowers' and thereby play a key role in exposing and preventing such breaches and in safeguarding the welfare of society. However, potential whistleblowers are often discouraged from reporting their concerns or suspicions for fear of retaliation. In this context, the importance of providing balanced and effective whistleblower protection is increasingly acknowledged at both Union and international level" [14].

The next section of this article summarizes important aspects of the directive [14] as a basis for discussion. Section 3 presents findings from the literature research and considers the main aspects of ethos as the basis for ethics and morality, using these as a way in to the subsequent discussion of Directive (EU) 2019/1937. Section 4 opens up this discussion to answer the question in the title of the paper, while section 5 sums up the arguments and looks at the prospects for further research activities in this area.

2. Directive (EU) 2019/1937 in a Nutshell

As set out in Article 2, Paragraph 1, of Directive (EU) 2019/1937 [14], breaches of Union law mean those that relate to the following material areas: public procurement; financial services and prevention of money laundering and terrorist financing; product and transport safety; protection of the environment; radiation protection and nuclear safety; food and feed safety, animal health and welfare; public health; consumer protection; protection of privacy and personal data, and the security of network and information systems. These areas of application thus affect the majority of critical infrastructures relating to IS in general, and to the IT Security Act in Germany [15], in particular, as well as the EU's General Data Protection Regulation (GDPR) [16]. In addition, breaches of the Union's financial interests and of various internal market regulations are included, especially if they aim to obtain a tax advantage that runs counter to the aim or purpose of the applicable corporate tax law [5].

Unlike EU regulations, such as the GDPR, which apply directly to the EU, EU directives need to be converted into national law. According to Article 2, Paragraph 2, the member states can extend the protection under national law with regard to areas or legal acts beyond the content of Directive (EU) 2019/1937 [14].

Article 3 lists the applications of Union or national law that are *not* affected by the directive [14]. This includes national security interests and defense aspects, protection of classified information; the protection of legal confidentiality obligations and medi-cal professional privilege; the secrecy of judicial deliberations; and rules on criminal procedure.

Article 4 of the directive—"Personal scope"—specifies the persons who can act as whistleblowers [14]. These are, for example, employees, the self-employed, shareholders, contractors, suppliers, and people whose employment relationship has already ended, as well as those who are still in the recruitment process. The measures to protect whistleblowers can also

apply to intermediaries, third parties, and legal entities.

Article 5 of the directive [14] clarifies in more detail the terms "breaches," "information on breaches," "report," "internal reporting," "external reporting," "public disclosure," "reporting person," "facilitator," "work-related context," "person concerned," and "retaliation." The data subject who committed the breach may also be a legal person, as well as a natural person [14]. The terms "follow-up," "feedback," and "competent authority" are likewise defined in Article 5.

Article 6 [14] sets out the conditions for protecting reporting persons, commonly called whistleblowers.

Article 8 of the directive [14] sets out the obligation to establish internal reporting channels and follow-up measures for legal entities in the private and public sectors. The Member States may exempt from this obligation municipalities with fewer than ten thousand inhabitants, or fewer than fifty employees, or other legal entities with fewer than fifty employees. Likewise, the "Member States may provide that internal reporting channels can be shared between municipalities or operated by joint municipal authorities in accordance with national law, provided that the shared internal reporting channels are distinct from and autonomous in relation to the relevant external reporting channels" [14].

According to Article 10 [14], reporting persons can also use external reporting channels after they have first reported information via internal channels. However, they can also submit reports on breaches directly via external reporting channels. As per Article 11 [14], the Member States are obliged to designate competent authorities that are empowered to receive such reports, provide feedback, and take appropriate follow-up measures. They shall provide these authorities with adequate resources. These external reporting channels should be independent and autonomous. Article 12 [14] lists the criteria that are in place to ensure independence and autonomy. In line with Article 14 of the directive [14], Member States should ensure that these competent authorities review their procedures for receiving reports and for follow-up measures on a regular basis: at minimum, every three years.

Article 15 [14] sets out the conditions for the right to protection under this directive for a reporting person who publicly discloses information.

Article 16 in Chapter V of the directive—"Provisions Applicable to Internal and External Reporting"—deals with the duty of confidentiality [14]. The following principles apply here:

1. "Member States shall ensure that the identity of the reporting person is not disclosed to anyone beyond the authorised staff members competent to receive or follow up on reports, without the explicit consent of that person. This shall also apply to any other information from which the identity of the reporting person may be directly or indirectly deduced.

2. By way of derogation from paragraph 1, the identity of the reporting person and any other information referred to in paragraph 1 may be disclosed only where this is a necessary and proportionate obligation imposed by Union or national law in the context of investigations by national authorities or judicial proceedings, including with a view to safeguarding the rights of defence of the person concerned.

3. Disclosures made pursuant to the derogation provided for in paragraph 2 shall be subject to appropriate safeguards under the applicable Union and national rules. In particular, reporting persons shall be informed before their identity is disclosed, unless such information would jeopardise the related investigations or judicial proceedings. When informing the reporting persons, the competent authority shall send them an explanation in writing of the reasons for the disclosure of the confidential data concerned.

4. Member States shall ensure that competent authorities that receive information on breaches that includes trade secrets do not use or disclose those trade secrets for purposes going beyond what is necessary for proper follow-up." [14]

As per Article 17 and in line with the EU GDPR, "personal data which are manifestly not relevant for the handling of a specific report shall not be collected or, if accidentally collected, shall be deleted without undue delay." [14] Article 18 of the directive [5] explains the obligation to document reports.

Article 19 in Chapter VI of the directive—"Protection Measures"—explains the prohibition of retaliation [14]. Accordingly,

the Member States shall take the necessary measures to prohibit any form of retaliation against whistleblowers and others as per Article 4. This includes, in particular, the following threats and attempts at retaliation:

(a) "suspension, lay-off, dismissal or equivalent measures;

(b) demotion or withholding of promotion;

(c) transfer of duties, change of location of place of work, reduction in wages, change in working hours;

(d) withholding of training;

(e) a negative performance assessment or employment reference;

(f) imposition or administering of any disciplinary measure, reprimand or other penalty, including a financial penalty;

(g) coercion, intimidation, harassment or ostracism;

(h) discrimination, disadvantageous or unfair treatment;

(i) failure to convert a temporary employment contract into a permanent one, where the worker had legitimate expectations that he or she would be offered permanent employment;

(j) failure to renew, or early termination of, a temporary employment contract;

(k) harm, including to the person's reputation, particularly in social media, or financial loss, including loss of business and loss of income;

(l) blacklisting on the basis of a sector or industry-wide informal or formal agreement, which may entail that the person will not, in the future, find employment in the sector or industry;

(m) early termination or cancellation of a contract for goods or services;

(n) cancellation of a licence or permit;

(o) psychiatric or medical referrals." [14]

In Article 20 [14]—"Measures of support"—the Member States shall ensure that the persons named in Article 4 have access to supportive measures: in particular, to comprehensive and independent information and advice on procedures against retaliation and on the rights of the person to whom the data belongs. A certificate must also be completed stating that the requirements for protection in accordance with this directive are met. Legal aid and legal advice are also available.

Article 21 goes into greater detail on the measures providing protection against retaliation. Accordingly, Member States shall take the necessary measures to ensure that the persons referred to in Article 4 are protected against retaliation [14]. These persons will have access to appropriate remedial measures against retaliation, including interim relief during ongoing legal proceedings in accordance with national law, and full reparation for the damage suffered. Furthermore, Article 21 states the following:

• Individuals cannot be held liable in any way for such reporting or disclosure assuming they had reasonable grounds to believe that reporting or disclosure of the information was necessary to detect a violation under this directive.

• Reporting persons (whistleblowers) cannot be held liable for obtaining or accessing information that has been reported or disclosed, unless the process of obtaining or accessing this information constituted a criminal offense in its own right. In the event that this does constitute a distinct criminal offense, criminal liability remains subject to national law.

• Any further possible liability of the whistleblower based on acts or omissions that are not related to the reporting or disclosure or are not necessary for the detection of a breach under this directive will continue to be subject to applicable Union or national law.

• In proceedings before a court or other authority that relate to a disadvantage suffered by the whistleblower and in which the whistleblower claims to have suffered this disadvantage as a result of his report or disclosure, it is presumed that the disadvantage was a reprisal in retaliation for the act of reporting or disclosure. In such cases, it is up to the person who took the prejudicial measure to demonstrate that it can be reasonably justified.

Article 22 [14] deals with measures to protect the persons concerned—i.e., the natural or legal persons who carried out the infringements. In accordance with the Charter, Member States shall ensure that the persons concerned can fully exercise their rights to an effective remedy and to a fair trial and the presumption of innocence, as well as their rights of defense, including the right to be heard and the right to inspect their files. In addition, the competent authorities ensure, in accordance with national law, that the identity of persons concerned is protected during an investigation triggered by the report or disclosure. The rules laid down for protecting the identity of whistleblowers also apply to protecting the identity of persons concerned.

Article 23 [14]—"Penalties"—defines the possible sanctions for natural or legal persons who are affected. They should be effective, proportionate, and dissuasive, as determined by the Member States. The underlying violations are as follows:

- Hindering or attempting to hinder reports;
- Taking reprisals against the persons referred to in Article 4;
- Bringing wanton legal proceedings against the persons referred to in Article 4;
- Violating the obligation under Article 16 to maintain the confidentiality of the identity of whistleblowers.

In addition, Member States shall lay down effective, proportionate, and dissuasive sanctions for whistleblowers who can be shown to have knowingly reported or disclosed false information.

Article 26 in Chapter 7—"Final Provisions"—defines the implementation and transition period [14]. Based on this, Member States shall put into force the laws, regulations, and administrative provisions necessary to comply with this directive by December 17, 2021. By way of derogation from this, the Member States shall, by December 17, 2023, put into force for legal persons with 50 to 249 employees the legal and administrative provisions that are necessary in order to comply with the obligation under Article 8 Paragraph 3 to set up internal reporting channels.

3. Literature Research

3.1. Findings to Clarify the Term "ethos"

Philosophy is not in vogue these days, as evidenced by mounting and possibly insurmountable global problems, amongst which IS is a critical and growing concern. However, in order to be able to assess the potential that Directive (EU) 2019/1937 [14] has to build a security and safety culture within a company, we must also hark back to philosophical principles. According to Schweppenhäuser (2019), the word *ethos* in Greek philosophy stands for custom and wont, for mores and convention within communities, as well as for character: in other words, for consideration, intelligence, and discernment [17]. Spaemann, meanwhile, states that "ethos is actually what teaches us about what we need and why" [18]. Schweppenhäuser refers to the Heraclitean maxim "Character is destiny" [17:151]. But the broad scope of the word makes it clear that ethos cannot be interpreted in solely individualistic terms. "Not only do individuals have an ethos but so too do communities and societies; their lived ethos has, since Hegel, […] been termed morality" [17]. Hähnel (2014) puts this in concrete terms, asserting that ethos as *ēthos* (ἔθος) means custom or wont, while ethos as *ēthos* (ἦθος) signifies mores: "Already in Plato, ethos as mores is brought to bear via ethos as wont" [19]. Citing Honnefelder, he states that ethos is "the entirety of dispositions, beliefs, and norms that, in the form of a more or less coherent, internally organized model, is viewed by an individual agent or by a social group as a guiding principle mandating good and proper action" [19]. "Are there criteria stipulating how we should behave, what choices we should make in order to live well or appropriately? Such criteria must be of a general kind that go beyond the individual. In other words, not merely 'How should I act in order to thrive?' but 'How should I act appropriately in relation to others?'" [17]. Hähnel (2014) points out that "without ethos—in the sense of mores—[…] our essential moral attitude is nothing more than an effusive, airy construct" [19]. He sees this kind of holistic ethos not as an object of contemplation but, like Spaemann (2002) [18], as "a form of normality, humane normality." [19] As Horne argues [10], ethos implies the general and core values of our existence, supplying answers to the questions of who we are, what we are about, and why. So, what really matters in our existence? The central question for Horne is the "why," leading him to incorporate ethos as a key factor in identifying the basis of an ethical system—otherwise, people will be floundering about in *technē* without any *epistēmē* [A:21].

In summary, we have three terms to distinguish: ethos, ethics, and morality. In human behavior, ethos is the basis, whereby

ethics are the guidelines that determine how the ethos is carried out. Morality defines the specifics, articulated as concrete rules. Hähnel (2014) identifies a more fundamental problem in the fact that "ethics" as reflection on what is moral is distinct from "ethos" as lived morality [19]. This leads him to ponder the idea that ethics as a philosophy is not outwardly concerned with bringing ethos to bear but is interested rather in explicating the inherent structures of this ethos [19]. For Schweppenhäuser (2019), ethics constitutes a theory that clarifies, on the one hand, what is beneficial and expedient on the personal level and, on the other, what our liabilities are in a social sense, what is equitable, and what is required on the common level [17]. According to him, all ethics have particular and universal aspects [17]. "As everybody knows, our ways of life have grown apart in the modern age, and value orientations have diversified. Individual ideas of happiness and the plurality of lifestyles have led to contrary rationales for moral concepts" [17].

Hornbacher (2006) points out that every human society takes its bearings from theoretical assumptions, rules, and moral concepts, "which may manifest unconsciously as a characteristic set of attitudes, an ethos, but are nonetheless an expression of a concept of humanity and the world as a whole that is publicly sanctioned in each case" [20]. For him, "ethics as a philosophical discipline and explicit theory of appropriate human action strives for the reflexive provision and normative determination of valid ethical principles, which—especially in the Enlightenment tradition—should not simply be an expression of local traditions but a rationally justifiable yardstick for human action in general" [20]. According to Hornbacher (2006), the goal of this ethics is therefore "not the assemblage and reproduction of empirical, culturally specific, and thus contingent moral concepts or ethical codes, but the formulation of universal principles or norms that can claim validity across cultural boundaries" [20]. Ethics as a philosophical and reflexive theory of human practice therefore differs from the habituated ethos, which is lived within the framework of a particular way of life [20].

Schweppenhäuser (2019) points out that Aristotle examined the connection between the moral integrity of the individual and their action in the community not only in his reflections on ethics and their relationship to political theory but also in his theory of rhetoric [17]. For Aristotle, rhetoric is the link between ethics and politics, between "private affairs" and the "public weal" [17]. "Little has changed about this in the age of audiovisual, digital mass media. Campaigns focused on persuasion in the public sphere still employ the logos strategy based on logic and content, the pathos strategy with its emotional orientation, and the ethos strategy, which connotes credibility" [17]. This takes on particular relevance in times of war but is not restricted to this. According to Derian (2005), for example, US foreign policy has always been a struggle between ethics and power, and when politics escalates into war, the first casualty is truth [21]: *the* truth, which is considered the core value to be strived for in attaining human fulfillment in philosophical discourses, social discussions, and individual relationships. However, "The love of truth," its pursuit, and "the search for truth," which takes priority over everything else, is a central feature of the research on ethos, as encapsulated by Horne (n.d.) [10].

Horne (2014) goes even further—for him, the survival of the Homo sapiens species depends upon learning and passing on to future generations quality knowledge [22]. He notes increasing corruption in this process, leading to ignorance, environmental destruction, and breakdown in community [22]. Horne (2014) identifies the dialectical interrelationship between *epistēmē* (theory) and *techne*̄ (practice) within the framework of ethos, pathos, and logos [22]. For him, this structure and process, as learning, ensure coherence in the necessary development of knowledge [22]. Learning (the dialectic between academia and education, if we are to adhere to the etymology) strives for coherence as its pathos, and virtue (i.e., the best that we are capable of as humans learning about meaning) as its ethos, while its logos (the conveying of knowledge)—in the coming fully cybernetic cycle—resides in telling the species that our very being is about our need to learn [22].

3.2 Specific findings on Ethics and Morality

Ethics goes beyond morality and looks for principles on the basis of which moral behavior can be justified, because conflicts of interest or loyalty—for example, who takes responsibility for mistakes—are important in decision making [23]. This involves an attempt to clarify what is good and bad, or right and wrong, and in this respect it is not value free. Ethics is concerned with the creation of moral value statements and adherence to them [3]. Morality is always present when people meet, because every decision has a rationale behind it and its own code of ethics [3]. Morality includes rules and norms as well as moral principles of behavior. According to Horne's ethos, ethics and morality are on an ascending scale of detail and scope—for him, ethics are the guidelines, the specific behaviors required to carry out the ethos, and morality is the resulting code of behavior, the rules [10] [22].

Three methods in particular are touted as identification measures in our work life [23]: first, the Sustainability Balanced Scorecard; second, the Social Return on Investment; and third, Social Marketing. These three terms are testimony to the

zeitgeist and are based on the values of the capitalist system. The vocabulary of "return on investment" and "social marketing" are indication of the idea that values can be commercially exploited—strictly speaking, they reveal the ethos. In addition, ethics research uses dilemma-based examples to identify a person's moral concepts. These examples are situations in which, whatever choice is made, someone suffers a disadvantage. Nina Himmer [24] asks in a newspaper article with the title "Philosophical Tutoring for Nerds" whether computer science and ethics belong together. The professors and lecturers she interviewed also affirm this and demand a kind of Hippocratic oath for their informatics subject [24]. This statement points to the crux of the whole problem of omitting ethos: science refers to a way of investigating, but without a guiding ethos and its implementation via ethics, it is like talking about the shape of a volume of water apart from the vessel (see [10]). IT specialists are primarily interested in how and which technology works, but only a few of them think about the consequences of its use—even though the technology impact assessment has long been a component of implementation decisions, and Article 35 of the GDPR [16] explicitly includes the promotion of a data protection impact assessment. Accordingly, project managers are advised not only to define the rules of the (IT) project but also to discuss what values the project team has in common [5].

Oftentimes in the literature, when dealing with dilemmas, no explicit reference is made to ethos, but only to ethics. In line with [3:1102], one can distinguish ethical aspects and conflicts of interest/loyalty according to system goals, process goals, and team goals:

- The ethical aspects of system goals are, for example, restoring trust, consequences of the product, fairness to the competition, and image preservation. Conflicts here could be living the company credo, compliance with the legal fundamentals, integrity, honesty with the customer, security, and sustainability.
- The ethical aspects of process goals are the truthfulness of the delivery results, generosity, intuition, respect, loyalty, and common sense. Other conflicts could relate to transparency of action toward stakeholders, order reliability, the escalation route, and plausibility.
- The ethical aspects of team goals are, for example, dealings with one another, trust in one another, understanding and solidarity with one another, crisis behavior, and project tactics. Further conflicts might involve capacity loyalty, the flow of information, moral behavior, decision making, and health.

Exacting demands are thus placed on project managers in terms of responsibility, competence, and integrity. According to [11], responsibility means that every project manager gives high priority to the common good as well as to the health and safety of each individual. Project managers strive to improve living conditions and the quality of the environment, are open-minded, and have tolerance toward other cultures [11]. They align their actions and decisions with the specific aim of ensuring the project's success for the client (Auftraggeber) [11]. It is recommended that project managers have the competence to carry out projects only when the complexity and consequences are not overlooked, and they weigh alternatives critically in order to do justice to social values [11]. But is that the reality? They should pay attention to freedom of action and base their decisions on the common good [11]. In addition, they should report openly and truthfully on conflicting goals and project problems and pay attention to fair cooperation and objective criticism [11]. In order to improve their own skills and knowledge, they need to engage in constant training themselves and in the process also create opportunities for personal professional development and training for their team [11]. The integrity of the project manager involves respecting the law and generally accepted social values wherever they are active in the world, while also consistently seeking to ward off harm to the common good and being ready to be accountable for what they have done [11]. In all their actions and decisions, project managers maintain their independence and neutrality, are loyal administrators of the client, maintain the confidentiality of information and protect copyrights, and strictly reject any form of unfair influence [11]. It is therefore important for the project manager to reflect on their sense of ethos, the way it underpins their ethics, and the moral code this produces. "'I am ethics'—ethics starts with everyone!" [12]. The core elements of responsible management are the principles of humanity and reciprocity, and the values truthfulness, partnership, justice, and non-violence have global validity [12]. "'Ethics is the new green.' True leadership is the triad of responsible behavior, ethical intent and sustainable results" [12], leading from business is business to business is social. By referring to social needs, this statement leads back to Horne's key question of "why" and the central importance of ethos as the starting point of an ethical system and the "love of truth" [10]. The ethical aspects of process goals are the truthfulness of the delivery results, generosity, intuition, respect, loyalty, and common sense.

Lucas Introna (2017) discusses phenomenological approaches to ethics and information technology (IT) [25]. Using historical

examples, he shows that phenomenology was used not only to answer questions in philosophical anthropology but also, for example, to deliver a devastating criticism of the classic program of artificial intelligence (AI). IT has become ubiquitous in a very real sense and its economic, organizational, and social benefits are generally uncontroversial [25]. According to Introna, the dispute is more often about how IT changes or transforms the social and, in particular, the ethical area. Regardless of the fact that the discussion focuses on whether IT creates new types of ethical problems that require a new ethical theory or whether the established ethical theory is sufficient, the debate, as per [25], tends to examine the guidelines that provide support in regulating or justifying behavior in respect of the negative effects of IT applications or IT implementations. The guidelines thus provide an opportunity to balance competing rights or competing values in the context of the effects of IT. "Furthermore, these debates are most often directed at an institutional level of discourse—i.e., with the intention of justifying the policies or conduct of governments, organizations, and individuals. In these debates on the impact of technology, ethicists are primarily conceived as presenting arguments for justifying a particular balance, of values or rights, over and against other possibilities within the context of specific uses or implementations of IT" [25]. For constructivists, the particular way in which values and interests are built into technology and practices, hidden in the logic of software algorithms or in hardware circuitry, is of ethical importance [25]. That is why they also demand ethical reflection as an integral part of the design process [25]. In addition, IT is usually not open to review by users or even experts [25]. "If information technology is political—i.e., it already includes/excludes certain interests—then it is also immediately ethical" [25].

Levina and Hasinoff (2017) critically examine the ethos of Silicon Valley and argue that, as a technology industry and a cultural force, Silicon Valley's practices and discourses reflect and produce particular social and economic investments in technology as a tool of empowerment and social change [26]. Their overall finding is that the ethos of Silicon Valley privileges disruption over sustainability, sharing economies over union labor, personalized access over public health, data over meaning, and security over freedom [26]. They analyze the ways this ethos extends beyond Silicon Valley itself and shapes the way we think about and act toward labor, security, sexuality, and health [26]. As such, Silicon Valley's technology products—as well as the way we think about them—affect the social, political, and economic conditions of everyday life [26].

As Buchanan and Zimmer (2018) argue, "Internet research ethics is a sub discipline that fits across many disciplines, ranging from social sciences, arts and humanities to medical/biomedical, and hard sciences" [2]. However, with the Internet acting as a technical doorway to an unimagined flood of information, it is important to ask how a discussion about the quality of knowledge and the search for truth can be implemented. As yet no quality seal has been introduced nor is there broad awareness of disinformation campaigns. Meanwhile, research shows that Internet users rely on a combination of factors such as design look, site structure, and usefulness of information when they judge web sites [27]. Warnick (2004) argues that this reliance on distributed credibility may be appropriate in a web environment where authorship, credentials, and information sources are often not readily available for examination [27]. But then, haven't we given up on the search for truth? Moreover, addressing user behavior in cyberspace is difficult. Suler's (1996) findings on the Internet indicate that several factors contribute to people being more relaxed, more open, and less inhibited [28]: "First, there is the feeling of anonymity that cyberspace encourages. Second, there is a false confidence generated by a delayed response to user actions. A further factor is the merger of fantasy and reality, which is reinforced by our perception that the imaginary characters we have created might actually exist, perhaps in a make-believe world that does not demand the same responsibilities as the real world" [28]. Suler's conclusion is that ordinary users can adopt rules and norms that are different to those they might apply in the physical world—they become imaginary people carrying out acts that have no real consequence in the physical world [28].

Nevertheless, "conceptually and historically, Internet research ethics is related to computer and information ethics and includes such ethical issues as participant knowledge and consent, data privacy, security, confidentiality, and integrity of data, intellectual property issues, and community, disciplinary, and professional standards or norms. Throughout the Internet's evolution, there has been debate [about] whether there are new ethical dilemmas emerging, or if the existing dilemmas are similar to dilemmas in other research realms" [2]. This covers "growing areas of ethical and methodological complexity, including personal identifiability, reputational risk and harm, notions of public space and public text, ownership, and longevity of data as they relate to Internet research" [2]. Big data is also increasingly playing a role in this assessment. "While the concept of big data is not new, and the term has been in technical discourses since the 1990s, the public awareness and response to big data research is much more recent" [2]. The paper by Nikiporets-Takigawa and Otiutsky (2019) provides a discussion on the understanding of information ethics as a research field that scrutinizes ethical problems of social communication in close connection with the analysis of the cyber informatization process [29].

[25] Note "ethical" not in the sense that it automatically behaves ethically, but in the sense that it is subject to the constraints of ethics.

The scientific study "Whistleblowing Report 2019" [1], which is based on an online survey of a third of small and medium-sized enterprises (SMEs) and two-thirds of large companies (with more than 250 employees) from Switzerland, France, Great Britain, and Germany, had the following results:

• Around 40 percent of the 1,400 companies examined were affected by grievances in 2018. The statistical analysis shows that large companies and international companies are more likely to be affected.

• More than half the companies examined (60 percent) have a reporting office outside of the hierarchically or professionally prescribed reporting line through which whistleblowers can report specific or suspected irregularities.

• One in three companies without a reporting office plans to introduce, or is discussing introducing, one in the next twelve months. The most important motives include the wish to avoid financial damage and improve the company's image. For SMEs in particular, the implementation of a reporting office has not yet been an issue, partly because it is not required by law.

• The financial damage uncovered by the reporting office is higher, the more broadly the reporting is communicated. The companies in the survey with specialized reporting channels, such as hotlines or call centers, mobile apps, social media, and web-based reporting systems, receive more reports. An average of fifty-two reports were received by reporting offices in 2018.

• The size of the company and its international cooperation are correlated both with the probability of being affected by grievances and with the amount of damage involved.

The IS culture in a company depends on the awareness and expertise of employees to conscientiously and considerately comply with the guidelines led by management. The study by Da Veiga et al. (2020), based on a survey of 512 people from different organizations, shows that scientific interpretations of the definitions and different aspects of information security culture are very diverse [30]. "Safety culture is a multidimensional phenomenon", as formulated by Pfaff et al. in 2009 [31]. Their main hypothesis, with regard to a healthcare organization, is that its safety culture strongly depends on its social capital, its communication culture, and its "error culture" [31]. The authors point out that safety culture is a characteristic of the organization and not of the individual, but that it manifests itself in the verbal and nonverbal behavior of the members of the organization and in their attitudes [31]. This also applies to a security culture in the institution and illustrates once again how closely security and safety are linked to human interaction.

4. Discussion

4.1. Lessons Learned

It is often postulated that the digitization of human interaction has led to progress and a host of new possibilities for humans. However, technology—and thus also IT or ICT—is not just an artifact or our relationship with it. According to Introna (2017), the artifact "is already an outcome of a particular 'technological' way of seeing and conducting ourselves in and towards the world" [25]. In addition, the move toward virtualization, for example with cyber communities, virtual education, virtual friendships, virtual organizations, virtual politics, etc.—and hence the transformation of the social area—obviously has an influence on our understanding of ethics [25]. This changing understanding affects institutions as well as individuals and society.

"Whistle blowers are a blessing for companies"—this is how Hauser et al. (2019) begin their whistleblowing report [1]. How many companies share this sentiment? While companies recognize that this allows risks to be recognized at an early stage and reputational damage averted, they still harbor reservations and there is no compliance culture in place. Moreover, there are a wide range of questions relating to IS. Not only is the clarification of technical and organizational problems necessary but legal, economic, and social answers also need to be found. IS is gaining importance in all institutions with increasing digitization. Linked to this is the extraordinary importance of the activity and competence of information security officers (ISOs) and the whole Security Management (ISM). However, the management of an organization already has a key responsibility in the initial phase of a security culture, both for establishing an information security management system (ISMS) and for business continuity management (BCM) [32]. If you want to sustainably establish new methods, awareness-raising measures, and training measures for IS in companies—as will be implemented, for example, in the author's new project, Awareness Laboratory SMEs (ALARM) Information Security, over the next three years [33]—you also have to deal with the topic ethics and whistleblowing. According to [30], "the ideal or strong information security culture can aid in minimizing

Note this is a well-established principle in software engineering and in requirements engineering

the threat of humans to information protection and thereby aid in reducing data breaches or incidents in organizations."

To summarize the European study [1], it can be said that some 50 percent of employee reports received by the companies examined have proven to be relevant and substantial. Anonymous reporting has—contrary to regularly expressed fears—no influence on the proportion of abusive reports [1]. According to Hauser et al. (2019), reporting offices are an effective instrument for disclosing illegal and unethical behavior and thus also make a decisive contribution to protecting the company's reputation [1]. Moreover, the instruments that are most commonly used are the most cost effective [1]: on the one hand, this is a clear signal from the management, who actively and openly address the issue and make it clear that illegal and unethical behavior will not be tolerated. On the other, the majority of the companies examined have drawn up a "Code of Conduct" that sets out the business principles and rules of conduct in written form. However, based on the author's experience with awareness-raising and training measures on IS, one can assume that long lists of rules do not have a lasting effect. Furthermore, if a single user action can jeopardize an entire security program, then the problem is the security program itself [34]. Security behavior is strongly influenced by the personal risk perception of the employees and these perceptions can be positively changed through continuous training [35]. In addition, informed and trained employees are considered a strength factor for the timely detection of security problems in the company [36]. However, the values relating to IT goods worthy of protection and IT security measures are different in different countries [6], as is the understanding of ethics.

The establishment of a security culture is undoubtedly necessary in institutions. However, the concept of security/safety culture is characterized by a great deal of openness (a "catch-all" term) [37]. Accordingly, the understanding of the concept of security/safety culture and its implications differs significantly not only worldwide but also nationally, and both between and within the various specialist disciplines. In actor-network theory, for example, security is conceived of as the stability of networks [38]. Accordingly, security culture examines interrelationships not only between people but also between people and technologies [38]. This analysis looks at so-called intermediate links (Zwischenglieder) and mediators (Mittler) in the interaction chain. Intermediate links ideally transfer an effect without any disruptive change, and mediators transform what is transferred in the process [38]. In this context, increasing security means replacing less predictable intermediaries (such as people) with more predictable intermediate links (such as digital actors). Technologies such as drones, detectors, and digital algorithms are increasingly helping to determine which specific, concrete situation is considered dangerous or non-dangerous. However, according to [38], such a man-machine monitoring network catering to the state's constantly growing need for security contains a paradox in that the increasing involvement of digital actors in ensuring our security requires increased levels of protection against these actors.

The overall results of the studies have concluded that the digital transformation of the labor market is an ongoing process that will have a profound overall effect on labor, albeit to varying extents when it comes to particular aspects of it [39]. In the logic of economic exploitation, phrases like "labor market" represent the commodification of humans, and the subsequent alienation should come as no surprise. However, diversity is spreading in the industrial economy. Koppetsch (2006), for example, argues that in the flexible forms of modern employment a new ethos, a new professional ideal has emerged that, in contrast to the traditional work ethic, is no longer based solely on values such as rationality, discipline, and control but is increasingly aligned with cultural ideals like creativity, autonomy, and personal development [40]. In addition, the role of the digital welfare state is becoming more complex. Thus, the challenges of upholding the "social contract" will become increasingly more difficult, as the ability to provide the same standard of welfare as today will likely decrease substantially [39].

Moreover, with the desired increase in digitization, many cities are also realizing that they have to include ethical aspects in their guidelines. An example here is Eindhoven's 2017 Smart Society Charter. The "IoT Architecture principles & guidelines" it sets out stipulate that "ethical aspects should be taken into account when extending practices into areas not addressed by current legislation" [41]. Eindhoven describes itself as a pioneer of the smart society, in which people are the most important thing, and is already facing significant changes and the dilemmas that the new technologies bring with them. The guidelines were written to safeguard the public interest, stimulate innovation, promote a sustainable ecosystem of partners and socially responsible business models, and ultimately ensure acceptance by the population. Acceptance and innovation are therefore the driving forces rather than a reflection of ethos. Another example is the UK government, whose commission continuously monitors the ethical standards that have existed since 2017 and currently publishes the progress made by local authorities on the recommendations for best practices in its 2021 report "Ethical Standards of Local Authorities" [42]. In addition, a comprehensive "Data Ethics Framework" has existed since 2020 to help public servants to understand

ethical considerations, take them into account in their projects, and encourage responsible innovation [43]. The framework refers to specific actions that can be taken at any stage of a public project to promote transparency, accountability, and fairness. The practical considerations are as follows [43]:

- Define and understand the public benefit and user need;
- Integrate diverse expertise;
- Comply with the law;
- Review the quality and limitations of the data;
- Evaluate and consider wider policy implication.

Governments and public authorities evidently want to create trust in current economic and social developments. The investigation of Cook et al. (2010) was motivated by the question "Can public trust in government be increased by expanding knowledge of the activities government already performs?" [44]. The analysis of a large Gallup survey of attitudes toward social security finds that recipients of personal social security statements gained more knowledge of, and confidence in, social security than non-recipients [44]. These results suggest that citizens' evaluations of government institutions echo, in part, the quality and quantity of information distributed to them [44]. The implication for future research on political trust and confidence is that "although an Athenian conclave of learned citizenry is not attainable, government institutions may be able to measurably improve the level of policy information and boost the public's evaluation of its programs" [44]. By adopting the Directive (EU) 2019/1937 [14], the public authorities are also imposing obligations on the private sector. Further research into the effects, opportunities, and limits of this as well as into people's awareness and ethical understanding of the complex application of technology in the social environment will be necessary.

The scope of Directive (EU) 2019/1937 [14] goes far beyond the issues of a security culture in institutions and affects Union law as a whole. As a common minimum standard, a high level of protection should be ensured for persons who report violations of Union law. However, it can also involve contractors, suppliers, and people whose employment relationship has already ended, as well as those who are still in the recruitment process. This should definitely be relevant in the IS area. Whistleblowers use external reporting channels to receive information about violations after they have first reported them via internal reporting channels. You can therefore submit reports directly via external reporting channels. How do the institutions then behave? They might also be subject to confidentiality obligations agreed between project partners—at universities, for example (see [45]). Are whistleblowers welcome in such situations? Are there any functioning reporting channels there? Can the reporting person be protected from reprisals? We all know current cases from the news. The discussion about this has only just begun. There are still no legal disputes within the EU, and we are still in the gray areas of assessment.

We are also facing another dilemma in the field of IS. Transparency and openness are prescribed as a means to comply with written statements on ethical values. At the same time, these qualities are actually only fully manifested in a few cases. Moreover, when levels of frustration, stress, intolerance, and bullying increase, execution of these qualities is jeopardized, because management has failed in its leadership role. If the social engineer becomes the employee's best friend, then the institution has lost. This is shown by the study of Enste et al. (2020), whose research confirmed the following three hypotheses [46]:

- Employees with a high degree of internal control belief achieve higher performance and strive for management and creative positions.
- Employees with a high degree of internal control belief are happier.
- Recognition and appreciation by the manager in connection with high levels of internal control belief promote the satisfaction of the employee.

The future viability of institutions depends to a large extent on the ability of their employees and the organization as a whole to learn and innovate. As Hartmann et al. (2006) point out, if the prescribed—or, in some places, collaboratively developed—guiding principles of an institution were actually put into practice, we would have a large number of institutions engaged in learning and probably sustainable as a result [47]. However, there is an enormous discrepancy between declared intentions and actual deeds [47]. This is why a profound change in individual and organizational behavior would need to be

initiated and a bundle of competencies imparted to make it possible to face new challenges [47]. Without this extensive ability to learn on the part of employees and the organization as a whole, the chances of companies, institutions, and societies surviving and devel-oping are rather low [47].

4.2. Some Ideas for Education and further Training

As Horne (2014) argues, "the world of learning is at a critical juncture" [22]. "Learning is not only for its own sake, but the way we apply it will determine whether we can address problems like environmental degradation, overpopulation, and resource allocation, all challenges to our species, itself" [22]. However, computer technologies that protect against threats have gained importance in the globally networked world, and the so-called human factor in information security was not given much attention for a long time. In addition, little is known about the attitudes and behavior of users toward this category of IT [48]. Comparative studies across different cultures are even rarer in this context, as Dinev et al. (2009) point out [48]. Their findings suggest that cultural factors should be considered in order to design effective IS policies, practices, and technologies in global networks where multiple cultures coexist [48].

The study by Horne et al. (2015) shows that when people think about a moral dilemma, they can successfully map multiple beliefs to the same situation [49]. When different beliefs result in different responses to the same situation, this suggests that the beliefs that are triggered are inconsistent, so one or more beliefs are revised to restore coherence [49]. Therefore, these results suggest that moral dilemmas can lead people to revise their beliefs by pitting inconsistent moral beliefs against one another [49]. This could also form a bridge for the necessary raising of awareness through communication and interaction.

The paper by Furnell et al. (2010) identifies the primary reasons why many contemporary business security awareness programs are ineffective [50]. Based on their investigations, individual actions are not only the cause of incidents, they are also the most important means of preventing, detecting, and resolving security problems [50]. People design, implement, operate, use, and abuse information systems, and they make mistakes that can be exploited by criminals [50]. However, with awareness and knowledge, they are also important in preventing a major security breach or managing an escalating crisis. The decisive realization of Furnell et al. (2010) is that the management of these risks and opportunities cannot be accomplished through the traditional security focus on policies, processes, and technologies [50]. Rather, new interventions are necessary for the new challenges in order to change people's consciousness, awareness, attitudes, and behavior. Unfortunately, best practices are not often judged by the appropriateness of their design and the effectiveness of their impact [50]. Furnell et al. (2010) explain that "some campaigns, especially those following a major incident, might even turn out to be counter-productive, as they encourage the establishment of a damaging blame culture which is not conducive to honest reporting of near misses and minor incidents" [50]. "A blame culture is dangerous because it promotes an ethos of lies, deception and avoidance of responsibility. Such a culture can by no means be regarded as an acceptable business practice." [50].

As Furnell et al. argue (2010), only few security practitioners can define precisely what a "better security culture" would be in their organizations. In practice, security culture means different things to different people [50], which is why we have a broad spectrum of possibilities when it comes to deciding the style of security culture we would prefer to encourage [50]. The main findings of Furnell et al. (2010) are that "inspiration is a more powerful, compelling, and longer-lasting lever than authority, but, in practice, the nature of most security cultures is largely determined by senior management reaction to major security incidents" [50]. "A culture of fear will certainly have some impact in making employees more cautious in managing information, but it will not eliminate the honest mistakes that are caused by overworked executives, inadequate checks and controls, and poor process design" [50]. "Over time, a security regime based on fear and punishment is likely to encourage the development of a 'blame culture' that undermines future cooperation, discourages risk taking and prevents honest reporting of factors that could contribute to further incidents" [50]. In fact, as Lacey (2009) points out, it is interesting to observe that the vast majority of mistakes that cause major security incidents are attributable to human factors that are not associated with bad behavior [51].

If the blame for an incident cannot be attributed to a single individual, where might the fault actually lie? "The logical response to a major breach is to investigate what went wrong, rather than who is to blame. The focus should be on identifying and addressing the underlying reason, rather than on the trigger of the incident, and the person who pulled it. But organizational responses are largely political, rather than logical, and such a response is neither obvious, nor easy, for most business managers. It demands a level of enlightenment on the nature of incidents, as well as a degree of confidence to challenge the instinctive corporate desire for a convenient scapegoat" [50]. Lacey (2009) argues: "Factors such as stress, lack of training

or supervision, and bad system or process design often lie behind many contemporary breaches. Management should not therefore seek to punish individuals for mistakes and omissions without first investigating the reasons for their errors" [51].

In addition, most analyses show that the initial effects of a campaign subside quickly and have little or no lasting effect on employee behavior [50]. Understanding organizational culture is not an easy task. However, according to Furnell et al. (2010), contemporary awareness campaigns fail because they are built on the best endeavors of managers rather than on sound principles of psychology and communications [50]. "Indeed, it is rare to witness a security awareness or behavior change program that is genuinely based on fact-finding, research and scientific principles" [50]. Furnell et. al (2010) suggest that changing how people operate in a working environment requires a good understanding of human behavior and some appreciation of best practices in marketing communications. Change programs will also need to be based on a clear strategy, a good understanding of key problem areas, a considered analysis of the root causes of incidents, and an appropriate set of remedial interventions [50]. Obviously, the previous methods for raising awareness are inadequate, neglecting the exchange of experience, communication, and learning interaction. Since improved understanding and the identification of inconsistencies can help people change their views and beliefs, it is clear that such insights can also be trained. As Callaos and Horne (2013) point out, scientific, technical, and societal problems require a multidisciplinary or interdisciplinary approach [52]: communication and interdisciplinarity are fundamental in modern scientific practice and also in the field of information security awareness (ISA). The project *Awareness Laboratory SMEs (ALARM) Information Security* [33] will attempt to provide the empirical evidence for the effectiveness of the new approach to workplace training.

5. Summary and Outlook

The paper's intention is to start a proper debate on the digital turn, the building of a security culture, and the dilemmas involved in long lists of regulations, which are no guarantee of commitment. The information security culture in institutions depends on the awareness and expertise of management and employees and relies on continuous communication and ongoing discussions to achieve concrete progress. The paper pursues the general question "How can this be achieved?" In common with Horne (2014) [22], one could also ask whether a free society will fail if it does not promote responsibility, social awareness, and ethical values. Answers to such a fundamental, pointed question, however, require extensive discussion between very different actors in society, which is beyond the scope of this publication.

The extensive literature research revealed many other questions, some of which, however, have remained unanswered and show the increased need for more interdisciplinary research. For some readers, the diverse literature may be an indication of the prevailing anarchy in IS, which is symbolic of a lack of social ethos and coherence. In any case, it becomes clear that an exchange that incorporates the philosophy of ethics is increasingly necessary in society: this has been neglected in the last decades, as can be seen in the insurmountable global problems we face. In particular, it is necessary to bring ethos, ethics, and morals into IT and IS and, by extension, into companies and institutions, as well as into the minds of engineers or people in general. This article covers a wide range of factors, and some might say that its focus is too wide. However, the author felt the need to demonstrate to engineers and other people the importance of ethos, ethics, and morals, and the possibilities presented by the Directive (EU) 2019/1937 [14] within their concrete work and life.

If one looks at the ethical concepts of cities and governments, the primary focus is on data ethics, and thus on the sensitive personal data of the population. Ultimately, in the course of extensive digitization, one would like to comply with the GDPR [16], which has been applicable in the EU since 2018. Data protection law is a law of prohibition based on the reservation of permission. The processing of personal data is only possible under certain conditions. With regard to the issues of interest in this paper, the GDPR provides the implementation and documentation of a data protection impact assessment before the start of any planned data processing. Moreover, it refers to "privacy by design" and "privacy by default," which means that data protection through technology design must be implemented at the time of planning with the help of technical and organizational measures. In this respect, the ethical ambitions of the Directive (EU) 2019/1937 [14] go beyond these concepts of data ethics.

Comprehensive digitization will seriously affect the status quo of work, shared values, and commitments. Mobile technologies and digital knowledge work are now of central importance in the industrialized nations. "There are no proper studies yet avail-able that show how this setting would affect the staff's productivity and/or morale, and more research into this space is encour-aged" [39]. How do we deal with other moral and ethical codes around the world in the future? It is important to note that the actions of individuals and companies must always be viewed in relation to their context, embedded in a specific time.

This frame of reference shapes individual and entrepreneurial behavior through rules, points of view, basic assumptions, and models of action that are often latent and implicit [47]. Ethics education in IS occurs not only in schools but also in workplaces. Therefore, scholars should examine the effectiveness of workplace ethics training.

Small to medium-sized companies collect, process, and use a great deal of sensitive data with the help of digital IT solutions, but they often underestimate the risks and threats posed by increasingly sophisticated attackers. Carelessness about information security and ignorance or violation of company guidelines or nonexistent information security guidelines constitute risks for companies of all types and sizes. The many vulnerabilities represent security deficiencies that can have delayed consequences for SMEs in the future. This is where the author's multidisciplinary research project Awareness Laboratory SME (ALARM) Information Security comes in [33]. A project like this, funded by the Federal Ministry of the Interior in Germany, which is developing a new overall scenario to raise awareness and support SMEs in the field of information security over a space of three years, must also take ethical issues into account. In this agile and participatory project, iteratively divided into three phases, an innovative process scenario for information security is developed with analog and digital experience-oriented scenarios as well as "on-site attacks" and other checks, such as awareness measurements, quizzes, and tests. The overall scenario should increase levels of much-needed emotional engagement in executives and employees and lead to targeted personnel development in SMEs, which is currently not yet widely available. To achieve this, IS is made tangible as an adjunct to increasingly digital work processes—at the same time, people are emotionally and actively involved in the development of measures. A sustainable and company-wide IS culture is being built up. This culture must contain a clarification of values—i.e., of ethos. Otherwise it will not work and will be pointless. The upcoming investigations have to uncover whether and how the management within companies understand this. It must also be made clear whether and how the EU whistleblower directive is being observed.

We will evaluate this process in the project ALARM Information Security and clarify the development in further scientific publications. One focus will be on the development of competencies and learning processes in the company. Bergmann et al. (2006) see competence as a problem-solving ability that develops particularly well in fear-free environments, where diverse learning opportunities are offered, routines are disrupted, and disturbances are initiated [53]. Practical experience and experimentation are particularly effective in the acquisition of skills [53]. Value competence is also included as a fundamental orientation on which one's own life, actions, and dealings with others are based. In addition, there is meta-competence as a universal competence. According to Bergmann et al. (2006), a meta-competent actor has the systemic ability to think and act, paired with a high degree of empathy and self-distance [53]. In connection with professional competence development, Bernien (1997) draws attention to the fact that different levels of learning should be distinguished [54]. He identifies four levels: individual learning, group learning, learning in organizations/regions, and learning across society [54:38]. Since people can change their views and beliefs after understanding and reflecting on inconsistencies, it is also possible to train this insight. To achieve that, our project's approach takes into account active communication, the participatory exchange of ideas and experience, and interactive learning processes.

"Hence, the time has come for a proper debate on the digital transformation of labor and what direction it should take in the future" [39]. The extent to which the EU directive can actually bring about a change in the way we work together is still unclear. Cases, assessments, and judgments on the EU directive must first be analyzed. However, one thing is already clear today: building an IS culture relies on a process of discussion! "Culture is primarily communication" [7]. Let us actively discuss the security and safety culture in our enterprise, company, and institution. Let us actively discuss this question in society and let us listen actively. In addition, more research is needed that includes the human side of technology's pervasive development, complete with its moral and ethical values. After all, the ISO 37002 standard on whistleblowing management systems has now been defined: this summarizes the organizational guidelines for the definition, implementation, maintenance, and improvement of an adequate and effective notice management system [55]. An effective system based on trust, impartiality, and protection should promote a culture of openness, transparency, and accountability. It remains to be seen how specific cases are made public and how whistleblowers are actually dealt with. To return to the question in the title of the paper: the EU Directive 2019/1937 [14] on whistleblowers can be used to build up a security and safety culture in institutions by giving greater weight than before to communication about regulations, the exchange of ideas and experience, and established reporting channels.

Acknowledgments

The author would like to thank the anonymous reviewers for their in-depth recommendations on several aspects of this paper.

Many thanks, too, to Simon Cowper for his detailed and professional proofreading of the text.

References

[1] Hauser, C., Hergovits, N., Blumer, H. (2019). Whistleblowing Report 2019. HTW Chur Verlag. Retrieved from: https://www.eqs.com/de/compliance-wissen/white-papers/whistleblowing-report-2019/. Accessed: October 25, 2020

[2] Buchanan, E. A., Zimmer, M. (2018). Internet Research Ethics, The Stanford Encyclopedia of Philosophy (Winter 2018 Edition), Edward N. Zalta (ed.). Retrieved from: https://plato.stanford.edu/archives/win2018/entries/ethics-inter-net-research/ . Accessed: October 31, 2020

[3] Schanz, R., Müller-Vorbrüggen, M. (2016). Ethics. *In*: GPM (ed.). Competence-based project management (PM3), manual for project work, qualification and certification, Volume 2, 8th edition, p. 1091-1103.

[4] Bundesamt für Sicherheit in der Informationstechnik (BSI) (ed.) (2020). Die Lage der IT-Sicherheit in Deutschland 2020. BSI-LB20/509, (September).

[5] Canham, M., Posey C., Bockelman, P. S. (2020). Confronting Information Security's Elephant, the Unintentional Insider Threat. In: Schmorrow D., Fidopiastis C. (eds) Augmented Cognition. Human Cognition and Behavior. HCII 2020. Lecture Notes in Computer Science, vol 12197. Springer, Cham. https://doi.org/10.1007/978-3-030-50439-7_22

[6] Pohlmann, N. (2016). Zur Entwicklung einer IT-Sicherheitskultur, DuD • Datenschutz und Datensicherheit 1 | 2016, p. 38- 42

[7] Gusy, C. (2010). Sicherheitskultur–Sicherheitspolitik–Sicherheitsrecht. Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft (KritV), 93 (2) 111-128. Retrieved from: https://www.nomos-elibrary.de/10.5771/2193-7869-2010-2-111/sicherheitskultur-sicherheitspolitik-sicherheitsrecht-jahrgang-93-2010-heft-2, Seite 111–211. Accessed: November 15, 2020

[8] https://www.th-wildau.de/hochschule/akademische-selbstverwaltung/ek/. Accessed: November 2, 2020

[9] Rat für Sozial- und Wirtschaftsdaten (RatSWD) (Ed.) (2017). Forschungsethische Grundsätze und Prüfverfahren in den Sozialund Wirtschaftswissenschaften, RatSWD Output, No. 9 (5), Rat für Sozial- und Wirtschaftsdaten (RatSWD), Berlin, Retrieved from: http://dx.doi.org/10.17620/02671.1 Accessed: January 25, 2021

[10] Horne, J. (2021). The philosophy of research. Retrieved from: https://www.academia.edu/38487203/The_Philosophy_of_Re-search_pdf. Accessed: January 17, 2021

[11] https://www.gpm-ipma.de/fileadmin/user_upload/ueber-uns/Organisation/Ethik-Kodex_der_GPM_deu.pdf. Accessed: October 31, 2020

[12] https://www.gpm-ipma.de/ueber_uns/aktuelles/detail/rueckblick_37_round_table_der_gpm_region_stuttgart.html. Accessed: October 31, 2020

[13] https://gi.de/ueber-uns/organisation/unsere-ethischen-leitlinien (in German), https://gi.de/ethicalguidelines (in English). Accessed: August 31, 2020

[14] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019L1937. Accessed: October 25, 2020

[15] https://www.bsi.bund.de/DE/Themen/KRITIS/IT-SiG/it_sig_node.html. Accessed: October 31, 2020

[16] GDPR, REGULATION (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. Retrieved from: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex%3A32016R0679. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679. Accessed: October 31, 2020. https://gdpr-info.eu/. Accessed: November 2, 2020

[17] Schweppenhäuser, G. (2019). Design, Philosophie und Medien. Wiesbaden: Springer VS

[18] Spaemann, Weltethos als 'Projekt', *In*: Spaemann, R. (2002). Grenzen: Zur ethischen Dimension des Handelns. Stuttgart: Klett-Cotta

[19] Hähnel, M. (2014). Das Ethos der Ethik: Zur Anthropologie der Tugend. Berlin: Springer VS

[20] Hornbacher, A. (2006). Globale Ethik für eine globale Welt? Ethische Dimensionen interkultureller Begegnung, 24 pages. Retrieved from: DOI: 10.14361/9783839404904-001. Accessed: October 31, 2020

[21] Derian, J. (2005). Imaging terror: logos, pathos and ethos. Third World Quarterly, 26(1), 23-37. Retrieved from: http://196.189.45.87/bitstream/123456789/18301/1/56.pdf#page=34. Accessed: January 10, 2021

[22] Horne, J. (2014). A Philosophy of Learning. *Systemics, Cybernetics and Informatics*, 12 (3) 103-107

[23] https://www.pmstatusreport.de/fileadmin/user_upload/Ethik_und_Moral_in_der_Projektarbeit.pdf. Accessed: October 28, 2020

[24] Himmer, N. (2019). Philosophische Nachhilfe für Nerds. Frankfurter Allgemeine Zeitung (FAZ online), January 4, 2019. Retrieved from: https://www.faz.net/aktuell/karriere-hochschule/informatik-und-ethik-gehoert-das-zusammen-15971263.html?service=printPreview. Accessed: September 14, 2020

[25] Introna, L. (2020). Phenomenological Approaches to Ethics and Information Technology, The Stanford Encyclopedia of Philosophy (Fall 2017 Edition), Edward N. Zalta (ed.). Retrieved from: https://plato.stanford.edu/archives/fall2017/entries/eth-ics-it-phenomenology/. Accessed: October 31, 2020.

[26] Levina, M., Hasinoff, A. A. (2017). The Silicon Valley ethos: Tech industry products, discourses, and practices. *Television & New Media*, 18 (6) 489-495.

[27] Warnick, B. (2004). Online ethos: Source credibility in an "authorless" environment. American Behavioral Scientist, 48 (2) 256-265

[28] Suler, J. (1996). The Psychology of Cyberspace World Wide Web. Retrieved from: http://www-usr.rider.edu/~suler/psycyber/psycyber.html. Accessed: January 26, 2021

[29] Nikiporets-Takigawa, G., and Otiutsky, G. (2019, June). On the Typology of the Information Ethos. *In*: International Conference on Digital Transformation and Global Society. Cham: Springer, p. 177-186

[30] Da Veiga, A., Astakhova, L.V., Botha, A., Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. Computers & Security, 92, 101713.

[31] Pfaff, H., Hammer, A., Ernstmann, N., Kowalski, C., Ommen, O. (2009). Sicherheitskultur: Definition, Modelle und Gestaltung. Zeitschrift für Evidenz, Fortbildung und Qualität im Gesundheitswesen, 103 (8) 493-497. Retrieved from: https://www.sciencedirect.com/science/article/pii/S1865921709002840. Accessed: October 25, 2020

[32] Scholl, M., and Ehrlich, E. (2020). Information Security Officer: Job profile, necessary qualifications, and awareness raising explained in a practical way. Frankfurt am Main: Buchwelten Verlag

[33] https://alarm.wildau.biz. Under construction. Accessed: November 23, 2020

[34] Winkler, I. (2017). The Human Exploitation Kill Chain (Video), RSA Conference. Retrieved from: https://www.rsaconference.com/events/us17/agenda/sessions/6682-The-Human-Exploitation-Kill-Chain%20RSA. Accessed: May 30, 2017

[35] Beyer, M., Ahmed, S., Doerlemann, K., Arnell, S., Parkin, S., Sasse, A., Passingham, N. (2016). Awareness is only the first step. A framework for progressive engagement of staff in cyber security. Hewlett Packard, Business white paper.

[36] Dark, M.J. (2006). Security Education, Training and Awareness from a Human Performance Technology Point of View, in M. E. Whitman, and H. J. Mattord (eds.), Readings and Cases in Management of Information Security, Course Technology, Mason, p. 86–104

[37] Lange, H.-J., Wendekamm, M., and Endreß, C. (2014). Dimensionen der Sicherheitskultur. Retrieved from: 10.1007/978-3-658-02321-8. Accessed: November 23, 2020

[38] Rauer, V. (2014). Interobjektivität: Sicherheitskultur aus Sicht der Akteur-Netzwerk-Theorie. Univ.-Bibliothek Frankfurt am Main. Republication Working Paper 14 (2013), in: Daase, Offermann, and Rauer (eds.), Sicherheitskultur. Soziale und politi-sche Praktiken der Gefahrenabwehr, Frankfurt/Main: Campus.. Retrieved from: http://www.sicherheitskultur.org/Work-ingPapers/14-Rauer.pdf. Accessed: October 25, 2020

[39] Larsson, A., Teigland, R. (eds.) (2020). The Digital Transformation of Labor, Taylor & Francis.

[40] Koppetsch, C. (2006). Das Ethos der Kreativen. Eine Studie zum Wandel von Arbeit und Identität am Beispiel der Werbeberufe. Konstanz/Köln: Herbert von Halem Verlagsgesellschaft mbH & Co. KG.

[41] https://data.eindhoven.nl/explore/dataset/eindhoven-smart-society-iot-charter/information/. Accessed: January 22, 2021

[42] https://www.gov.uk/government/publications/local-government-ethical-standards-progress-made-against-best-practice-

recommendations. Accessed: January 23, 2021

[43] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/923108/Data_Ethics_Framework_2020.pdf. Accessed: January 23, 2021

[44] Cook, F. L., Jacobs, L. R., Kim, D. (2010). Trusting what you know: Information, knowledge, and confidence in Social Security. *The Journal of Politics*, 72 (2) 397-412.

[45] TH Wildau (2020). Non-disclosure Agreement. Retrieved from: https://www.th-wildau.de/files/2_Dokumente/Formulare-Antraege/Beschaeftigte/Passwortgeschuetzt/GeheimhaltungsvereinbarungInklBelehrung_Deu-Eng_Fassung_04-2020.docx. Accessed: November 11, 2020

[46] Enste, D., Kürten, L., Suling, L., Orth, A. K. (2020). Digitalisierung und mitarbeiterorientierte Führung: Die Bedeutung der Kontrollüberzeugung für die Personalpolitik, IW-Analysen, No. 135, ISBN 978-3-602-45630-7, Institut der deutschen Wirtschaft (IW), Köln. This Version is available at: http://hdl.handle.net/10419/214160. Accessed: October 25, 2020

[47] Hartmann, D. M., Brentel, H., Rohn, H. (2006). Lern- und Innovationsfähigkeit von Unternehmen und Organisationen. Retrieved from: http://nbn-resolving.de/urn:nbn:de:kobv:109-opus-11415, Wuppertal-Inst. für Klima, Umwelt, Energie. Accessed: November 15, 2020.

[48] Dinev, T., Goo, J., Hu, Q., Nam, K. (2009). User behaviour towards protective information technologies: the role of national cultural differences. *Information Systems Journal*, 19 (4) 391-412

[49] Horne, Z., Powell, D., Hummel, J. (2015). A single counterexample leads to moral belief revision. Cognitive science, 39 (8) 1950-1964

[50] Furnell, S. M., Clarke, N., Lacey, D. (2010). Understanding and transforming organizational security culture. Information Management & Computer Security. *Information Management & Computer Security*, 18 (1) 4-13.

[51] Lacey, D. (2009). Managing the Human Factor in Information Security, London: Wiley.

[52] Callaos, N., Horne, J. (2013). Interdisciplinary communication. Journal of Systemics, Cybernetics and Informatics, 11 (9) 23-31. Retrieved from: http://www.iiis.org/Nagib-Callaos/Interdisciplinary-Communication/Interdisciplinary%20Communication%20-%20Short%20Draft.pdf. Accessed: January 17, 2021

[53] Bergmann, Gustav., Daub, Jürgen., Meurer, Gerd (2006). Metakompetenzen und Kompetenzentwicklung, Teil II: Metakompetenzen und Kompetenzentwicklung in systemisch-relationaler Sicht. Selbstorganisationsmodelle und die Wirklichkeit von Organisationen, QUEM-report, No. 95/Teil 2, Arbeitsgemeinschaft Betriebliche Weiterbildungsforschung (ABWF), Berlin. This Version is available at: http://hdl.handle.net/10419/105487

[54] Bernien, M. (1997). Anforderungen an eine qualitative und quantitative Darstellung der beruflichen Kompetenzentwicklung. *In*: Arbeitsgemeinschaft Qualifikations-Entwicklungs-Management (Hrsg.): Kompetenzentwicklung ’97: Berufliche Weiterbildung in der Transformation – Fakten und Visionen. Münster, New York, München, Berlin 1997, p 17-83

[55] E DIN ISO 37002:2020-08 [ISO / DIS 37002:2020(E)]: Whistleblowing management systems – Guidelines, Text in German and English, August 2020.