Why Trustworthiness is the Cornerstone of Digitalization

Ulla Coester and Norbert Pohlmann

Abstract The importance of trust is generally recognized. Yet the principle of "everything in moderation" also applies, meaning, in short: trust is good, but control is better. This insight has wide-ranging implications, especially in the current discussion surrounding digitalization. But what happens when it is no longer possible to control an IT or AI solution due to its complexity? At first glance, there are only two options: either refrain from using the technology altogether or simply trust the provider. But neither alternative is suited to the task of advancing digitalization in a meaningful way. On the contrary, providers and users must cooperate on equal terms in order to shape the digital transformation together in a responsible manner. This requires users to trust the technology and the provider. Due to the strong interdependence between trust and trustworthiness, trustworthiness is the cornerstone of the digital transformation.

Keywords Trust · Trustworthiness · Digitalization · Complexity

1 Building Trust in Digitalization

1.1 Building Trust: Reducing Complexity

In the context of digitalization, a new form of interdependency has arisen between manufacturers or provider and users and also user companies due to the increasing complexity intrinsic to the use of new technologies. This results in consequences for both parties: On the one hand, it affects the users' competence in decision-making, and on the other, it limits the options available to the providers. Neither of the two

U. Coester · N. Pohlmann (✉)
Institute for Internet Security—if(is), Westphalian University of Applied Sciences, Neidenburger Strasse 43, 45897 Gelsenkirchen, Germany
e-mail: pohlmann@internet-sicherheit.de

U. Coester
e-mail: coester@internet-sicherheit.de

U. Schmuntzsch et al. (eds.), *New Digital Work II*,
https://doi.org/10.1007/978-3-031-69994-8_10

parties has full sovereignty in the sense of freedom of action, because every action of the respective party has consequences. In practical terms, this means that users may be required to disclose more data when using services, even if they do not want to, and their data may be used in ways they cannot control. Conversely, users now have more opportunities to monitor activities of providers.

Efforts to improve the quality of this interrelationship are therefore essential, especially those focused on the acceptance of innovative technologies in general and AI solutions in particular. The necessity of such efforts becomes particularly clear in light of the fact that innovative technologies—and thus the entire internet/IT infrastructure—have not only become more and more complex but also increasingly opaque. This results in a serious dilemma: Increasing use is enforced—whether intended or involuntary—while knowledge about the background of and interrelationships within these structures is decreasing. This dilemma has the potential to produce behavioral dichotomy in users: either disproportionate rejection of the technology and corresponding services or blind trust. Both behaviors are counterproductive in terms of value-creating digitalization. Although the latter does not preclude use in general, it prevents meaningful use of new applications or innovative services, since use is neither based on a high level of decision-making competence nor on the sovereignty, or autonomy, of the user.

However, since trust has fundamentally positive connotations—according to sociologist Niklas Luhmann, trust is a mechanism for reducing complexity (Luhmann 1968), i.e., it makes life easier—providers should direct their activities toward building a relationship of trust with their users. At first glance, this idea might seem trivial. Yet while trust may reduce complexity, the construct of "trust" is in itself complex, since the collective conditions under which it manifests are highly exacting. Thus, it is necessary to examine this concept in more detail.

1.2 Building Trust: The User's Perspective

According to Luhmann (Luhmann 2000), trust enables an optimistic view of the future, although individuals possess neither sufficient information nor the necessary control to justify this optimism. Trust can therefore be described as an adaptive strategy that helps individuals retain their capacity for action in a world characterized by uncertainty. Put simply, according to Luhmann (Luhmann 2000), trust is a mechanism for reducing complexity. Generally, human beings possess varying capacities for trust, but this capacity differs among individuals. In principle, there are various concepts that can be used to explain the emergence of trust, such as "trust based on routine" (Pohlmann 2022). In the context of digitalization, the model of "trust based on reason" is particularly pertinent. Establishing this type of trust depends on the one hand, on a person's benefit, interests, and preferences and, on the other hand, on their ability to process information and to recognize trustworthy interaction partners based on certain criteria. According to a widely used model (Möllering 2006), these criteria include, for example, competence, benevolence, and integrity of the trusted party.

Rational trust thus constitutes a person's attribution of reasons for trustworthiness to, for example, a particular provider. In the context of digitalization, this concept could be applied as follows: The user must receive reliable signals of trustworthiness regarding the provider's competence, goodwill, and integrity.

1.3 Building Trust: Change of Perspective to AI Provider

Trust—also in the context of digitalization, as mentioned above—can only be understood as a positive behavior if it is not blind and naive. This assumption is complicated by the fact that users must first trust in outside expertise because they are unaware of the capabilities, knowledge, and intention of the provider in question. Therefore, first and foremost, it is crucial to dispel the user's belief that the provider's interests have been placed above their own, or that a provider could behave opportunistically. Providers should recognize this as their duty—not least because this allows them to develop a relationship of trust with their users. In the context of digitalization, we could thus posit: The provider must prove that the user can trust them.

1.4 Building Trust: Law Versus Moral Philosophy/Ethics

In principle, it could be argued that between existing rules and regulations (laws) and those that will come into force in the foreseeable future, enough is already being done to nurture trust. But upon closer inspection, laws alone are insufficient because it may be possible for providers to develop and deploy AI that, while technically legal, is nevertheless illegitimate, because it ignores the interests of the user, serving only one-sided corporate interests.

In order to build trust, it is crucial to preclude mistrust. For providers, this necessitates increased transparency, especially relating to AI. In other words, providers must provide users with all the information they need to be able to build trust and thus achieve digital sovereignty as described above. Therefore, it is particularly important for AI provider to openly address how their actions relate to the interests of their customers—above and beyond any legal requirements (Fig. 1). Self-limitation, defined as "the ability to limit one's own freedom, whether in the form of external expectations or in the form of one's own actions, in such a way that the use of this freedom does not result in harm" (Suchanek 2021), is one method by which providers express respect for their customers. In terms of digitalization, this requires a consistent sense of responsibility on the part of the provider—starting with management strategy and ending with the developer, who is thus obliged to deliver an AI solution that is fair, transparent, and explainable. This rule could be expressed as follows: To build trust, providers should exercise transparency by openly presenting their organizational modalities and corresponding AI solutions within the framework of a "provider commitment" and by agreeing to adhere to these principles. As a caveat

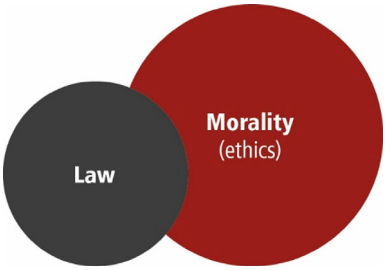

Fig. 1 Law and moral philosophy (own illustration)

to this rule, however, it is essential to maintain a degree of moderation with regard to transparency, because "transparency describes only the provision of information and does not necessarily result in understanding. In fact, too much information can limit comprehension." (DENKIMPULS DIGITALE ETHIK).

2 Approach: Trustworthiness Platform—Building Trust to Leverage the Potential of Digitalization

2.1 Structure of the Model of Trustworthiness

The relationships for building trust are illustrated in the model of trustworthiness (Fig. 2) and elucidated below based on each individual aspect (Coester and Pohlmann).

2.2 Definitions

Trust, trust giver, and trust receiver: Among other factors, trust relies on a subjective conviction of the correctness of actions. In principle, trust is necessary to reduce complexity and is thus required whenever the user is confronted with an uncertain or insecure situation or when the outcome of an action may involve risk. The trust giver's (user's) "ability to allow" themselves to trust a trust receiver (AI company) therefore equates to their willingness to refrain from questioning the respective trust receiver and, correspondingly, to expose themselves to a certain degree of risk.

Institutional trust: A basic requirement in encouraging people to use AI solutions is the promise of added value. Conversely, this means that if users do not obtain added value from using the AI solution, they are more critical in their assessment and thus less willing to adopt the respective solution. AI providers must also take additional steps to encourage users to extend their capacity to trust AI solutions. This can be achieved by transferring interpersonal trust—i.e., the relationship of trust that develops between people based on individual criteria—to AI solutions. The basic

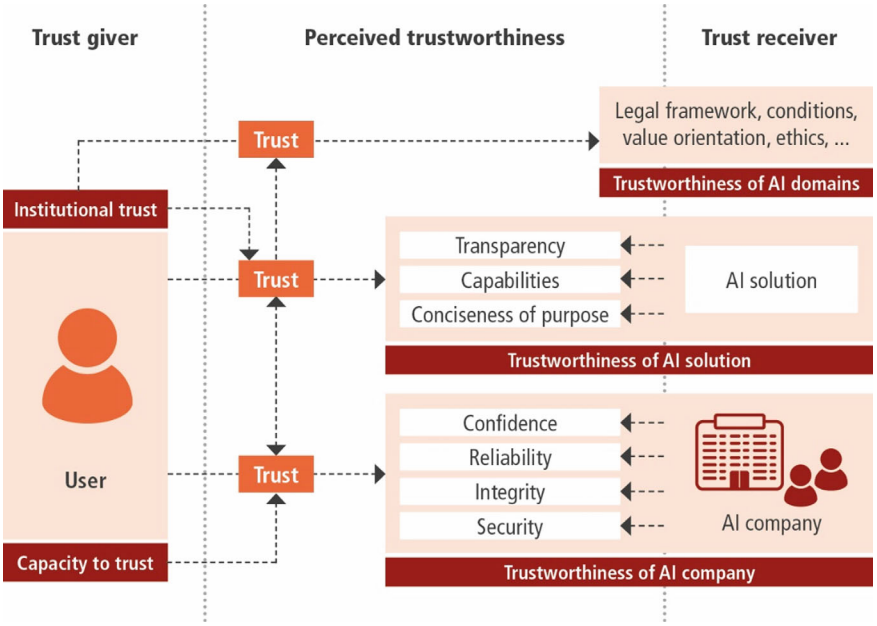

Fig. 2 Model of trustworthiness (own illustration)

idea behind this is that the providers present themselves as trustworthy so that the users can transfer their trust to them based on an assumed similarity.

Perceived trustworthiness: The concept of trustworthiness is based on the assumption that it is possible to rely on some specific aspect. As a rule, perceived trustworthiness is based on the apparent functionalities of the AI solution and measures taken by the AI provider (trustworthiness aspects). This can be demonstrated by not asking for all of the information about a person, but only the details that are necessary.

Trustworthiness: Trustworthiness is based on the assumption that it is possible to rely on given information, solutions, or actors. Presenting the trustworthy aspects of AI solutions as well as those of the provider company as a whole fosters user trust. Evidence of this can be provided in the form of a company commitment.

AI company: An AI company is a manufacturer or provider of AI technologies, products, or services. These individual categories are referred to collectively as AI solutions.

Users: Users include all parties who use AI technologies, products, or services, including user companies.

AI solution: In the context of artificial intelligence, an AI solution is any application that utilizes artificial intelligence mechanisms or an artificial intelligence system.

3 Trustworthiness of AI Domains

It is generally advantageous for providers to act independently in order to generate competitive advantages based on user-orientated policies and decisions. Yet it can be difficult or even impossible to assume a pioneering role and thereby shape the market. In many cases, the trustworthiness of an individual provider is insufficient to create a general level of trust in, e.g., an innovative approach to fundamental AI solutions. Therefore, AI providers must contribute to the trustworthiness of overarching AI domains. In other words, it can sometimes be advantageous to create value or implement value concepts collaboratively with other manufacturers. In this way, providers may contribute to the development of the entire industry or domain, thereby promoting the successful introduction of new business models or technologies. In principle, there are several options for establishing the trustworthiness of (new) technologies and AI solutions. The following is a list of possible examples related to domains:

Creating framework conditions: *The state creates legal frameworks by specifying how providers are expected to design the use of technology and AI solutions within the context of a given domain. One example of this is the EU Artificial Intelligence Act (AI Act).*

Motivating ecosystems: *One example in this area is the Gaia-X industry consortium. Demonstrating trustworthiness is not only a relevant issue for new IT technologies; even for established technologies, standards must be redefined periodically to align with shifting values, and new standards must be implemented accordingly. According to Gaia-X principles, providers must guarantee that their AI solutions comply with European law and ensure data portability while adhering to the strictest IT security standards and offering transparency about data usage.*

4 Trustworthiness of AI Solutions

For AI providers to transfer trust to their AI solutions in a dedicated manner, they must account for other aspects—apart from artificial intelligence—that play a role in determining perceived trustworthiness, including transparency, performance, and conciseness of purpose. Only by considering all these aspects can providers nurture user trust in their AI solutions.

4.1 Trustworthiness Aspect: Transparency of an AI Solution

The principal benefit of embracing transparency is that this practice demonstrates the AI providers' willingness to seriously consider their users' needs and to communicate openly. By no means does this involve disclosing every detail of the AI solution or

the associated business activities. Rather, it means that users are provided with all the relevant information they need to make a sound decision about the trustworthiness of the AI solution in question. Consequently, quality of information plays a decisive role: It should be participatory and balanced, meaning that it should account for the interests of all parties in equal measure. In the past, this form of communication was not necessary. However, due to the growing complexity of current solutions, such transparency is now essential to increase the users' willingness to adopt AI solutions. This situation illustrates the interplay between trust and trustworthiness: An AI provider depends on the acceptance of its users. At the same time, due to the potential of smart applications to influence users, it becomes increasingly important to demonstrate respect for the users' need for sovereignty and privacy.

In depth instruction for use for an AI solution: *One way of ensuring transparency is, e.g., to provide—preferable as a package insert—an instruction leaflet detailing the potential effects of the AI-based application and how it can be controlled. This insert should also include information on the risks of use and how users can avoid or mitigate potential problems.*

4.2 Trustworthiness Aspect: Capabilities of an AI Solution

The capabilities of an AI solution are those parameters that the user can immediately comprehend and control. Therefore, the measurable criteria by which the user evaluates the AI solution are a product of the extent to which users feel supported in achieving their intended purpose and the suitability of the AI solution for their needs. Reliability and predictability are among the relevant evaluation criteria here. It is also important for the AI provider's expertise to be reflected in the capabilities of its AI solution. If a solution lacks capabilities, this ultimately reflects strategic errors or inadequate expertise on the part of the provider that produced it. This example demonstrates both the connection and interplay between the trustworthiness of the AI solution and that of the AI provider itself. The usability or performance of the AI solution, among other factors, can serve as an evaluation benchmark for users.

Performance of an AI solution: *How precise are the results, how high is the quality of the respective analyses, and how quickly can models be adapted to ensure that they remain up to date.*

4.3 Trustworthiness Aspect: Conciseness of Purpose of an AI Solution

Whether or not an AI solution can be said to have conciseness of purpose becomes apparent when examining the intended use of the AI solution. To ensure its solution has a conciseness of purpose, AI providers must precisely define the function and

intention of the AI solution during development. Accordingly, the intended use of the AI solution should be clear to the user. For this reason, it is important to ensure that the purpose of the AI solution and the use of its characteristic features can be easily and immediately understood. Yet this does not imply that achieving conciseness for purpose requires a low level of functionality. Furthermore, providers must openly communicate any relevant changes or extensions to the AI solution, especially if these alterations affect the users' ability to identify the originally intended use. If, in addition to the actual application, an AI solution includes supplemental functions designed solely for the interests of the AI provider or third parties, these functions must also be clearly presented and described.

Disclosure of the business model: If sensitive user data is collected under the "pay with personal data" business model and used for individualized advertising and/or sold to third parties for profit, providers must clearly communicate this intended use.

5 The Trustworthiness of AI Providers

When users weigh up whether or not to use new IT technologies, the features of the respective AI solution are not the only factors involved in their decision. The AI providers' reputation also plays an important role. At present, it is apparent that user trust in IT technologies, applications, and services is not (yet) fully justified. Therefore, providers are required to meet additional conditions to increase their level of trustworthiness. To this end, AI providers must disclose their strategies to the outside world. In practical terms, this means aligning their actions with four trustworthiness aspects: confidence, reliability, integrity, and security. These factors allow users to rationally assess a provider's trustworthiness and quickly and easily evaluate the associated parameters.

5.1 Trustworthiness Aspect: Confidence in an AI Provider

Confidence is one of the key factors to trustworthiness. Generally speaking, with regard to functionality, confidence can be generated by providers with the capability and means to provide reliable, secure AI technology, services, and applications. It is important for providers to develop a strategy to address this aspect and then document it in a general confidence guideline that apply to all employees. For this purpose, among others, providers must create a concept defining the parameters to be fulfilled. The following parameters are of key importance here:

Employees: *Parameters pertaining to employee education, certification, and further training: Have the employees studied mathematics, computer science with a focus on artificial intelligence, or data science, or have they received further training*

in those fields; what experience do they have in the area of AI; what additional skill do they have?

Quality standards: *Parameters for development and production: Description of the development process, definition of the accompanying quality assurance process, including implementation and specification of life cycle management criteria.*

5.2 Trustworthiness Aspect: Reliability of the AI Provider

Reliability means that AI solutions execute only those processes that users desire or expect and that they do so with as close to 100% reliability as possible. Reliability thus implies that AI providers are fundamentally benevolent, meaning that they act in the best interest of their users, i.e., they focus primarily on their users' needs rather than on their own provider interests. One example of benevolent behavior would be for a provider to refrain from instrumentalizing obvious weaknesses of their users—and thus causing harm—to gain a (financial) advantage. For instance, a provider might choose to exploit a customer's preference for high-value branded products: Based on a user's buying behavior, he is placed in a particular category and regularly offered expensive products without a discount. However, given that no provider is perfect, cultivating reliability requires a willingness on the part of the provider to continue developing. In order to compensate for their existing deficits, providers must implement mechanisms that allow them to continuously and proactively improve their reliability and demonstrate this development to users. Ideally, user confidence should precisely mirror the actual reliability of the AI provider or the AI solution. Conversely, the AI providers risk damaging or losing their trustworthiness entirely if their actions are inconsistent with their public image. How will AI providers have to address this issue in the future?

What criteria should they include in their reliability management policy? The following parameters are key to reliability management:

Act cooperatively *in order to more effectively identify the real needs of the user and provide individual support when problems arise. Assuming overall responsibility in the event of damage or issuing recalls if problems are identified are examples of cooperative behavior. The AI provider must inform its users immediately—by direct means, if possible—should serious vulnerabilities be identified. When such information is preemptively published by third parties, for example* via *social media or the trade press, this reduces the trustworthiness of the AI provider.*

Act responsibly *to create added value for users through the correct use of functions that benefit the user. In general, in the context of AI solutions, acting responsibly means fulfilling all specifications required to ensure that input data is of high quality. Data must be complete, representative, and correct. The AI provider should have a single person in the organization whose responsibility it is to ensure that all necessary measures are taken to guarantee that these criteria are met (*Coester and Pohlmann 2020*).*

*Yet, data selection is not the only key factor; responsible handling is also essential. Some AI solutions may require it to start a debate as to whether the data analysis involved is truly in society's best interest. For example, what if Google Street View were used to predict the likelihood of people becoming involved in accidents based on where they live in order to derive more cost-effective insurance policies? Indeed, as the research team under Łukasz Kidziński of Stanford University and Kinga Kita-Wojciechowska from the University of Warsaw discovered, the location variable turned out to be a surprisingly good indicator of accident likelihood (*Coester 2020*).*

5.3 Trustworthiness Aspect: Integrity of the AI Provider

AI providers demonstrate integrity by considering all influencing factors that are relevant to trustworthiness, paying particular attention to the ethical dimensions. This means that, as a trust receiver, an AI provider must be capable of fulfilling all promises made, willing to consistently keep them, and prepared to observe social norms and values.

The ethical orientation of AI providers will be subject to even greater scrutiny in the future. Various studies corroborate this point. In one such example, it was found that 93% of users in Germany demand ethically responsible use of IT technology. Therefore, integrity should be viewed as an essential tenet of all business activities. One-dimensional, purely technically-oriented mindsets that disregard ethical considerations and values are poised to become less and less profitable—or may only prove profitable at all in the short term. This may be explained by the volatility of user behavior, which is subject to rapid influence by negative events or social media posts. Another key aspect to consider in this context is the variability in trust between individual users, a factor that renders general attitudes relatively difficult to assess. Therefore, one of the most important steps for AI provider is to draft an integrity maxim that includes a clear affirmation of their business model and other factors specific for provider. This maxim must address all relevant ethical considerations. Some applicable considerations to keep here in mind are:

Privacy protection: *This includes, on the one hand, responsible handling of customer data, such as immediate deletion when it is no longer needed, and protecting this data through encryption. In addition, it encompasses the commitment to refrain from exploiting user data for additional commercial purposes.*

Accountability: *One of the key aspects of accountability is ensuring the verifiability of the quality of AI solutions. In addition, it should be mandatory for providers to review the technologies they use and disclose any issues with the potential to negatively affect society.*

Responsible use of AI: *This includes, among other things, that providers do everything in their power to protect both individual users and society from harm, i.e., providers must not prioritize profit over human wellbeing. In other words, providers must avoid the behavior attributed to Facebook by a former employee during a hearing before the U.S. Congress: "The providers' leadership knows how to make*

*Facebook and Instagram safer but won't make the necessary changes because they have put their astronomical profits before people." She further emphasized that Facebook's actions carry major ramifications for democracy and society, claiming that the provider relaxed its misinformation filters following the 2020 US election to attract more users (*Tagesschau*).*

5.4 Trustworthiness Aspect: Security of the AI Provider

Recognizing the importance of cybersecurity and implementing the appropriate measures theoretically ensures that AI solutions can be used on the internet at low risk. Yet, this scenario remains aspirational, given that ransomware and DDoS, among other security issues, are commonplace. Some AI solutions or services used today do not offer the level of trustworthiness required to handle critical business processes securely. AI providers therefore require an adequate and well-defined IT security policy to guarantee the best possible protection—during the development process and later when the customers are using the AI solution. Because users (as well as user companies) are often not equipped to protect themselves adequately, AI providers must continuously ensure that their AI solutions are up to date concerning security. The following measures, among others, are critical in the context of security:

Presentation of cybersecurity measures used: *The AI provider must demonstrate the actions they are taking to protect both the AI solution and their own company from cybersecurity risks.*

Regular review of products and the AI provider itself: *The aim of this measure is to actively and continuously identify vulnerabilities with the help of penetration tests, red teams, and bug bounty programs designed to eliminate security vulnerabilities as quickly as possible. Systems are then updated before these vulnerabilities can be leveraged for attacks. This applies to both proprietary AI solutions as well as to the AI providers themselves and their suppliers. This makes it possible to maintain a high level of security—which is also verifiable for the user—throughout the ongoing development process.*

6 Conclusion: Trustworthiness as a Competitive Advantage

There is a crisis of trust—this fact is undeniable: "Eighty percent of Germans currently have little or no trust in the major digital corporations. This was the finding of a survey of 5,000 internet users in Germany conducted by the opinion research institute Civey on behalf of Next Conference" (Absatzwirtschaft).

The negative response to the Cambridge Analytica scandal, for example, or the current barrage of fierce media criticism leveled against Instagram clearly demonstrates the effects of negligent conduct. In other words, a responsible approach is key, especially in an international context. By demonstrating responsible behavior

alone, European companies can stand out from Asian and American AI providers, who often neglect this responsibility because this approach does not (yet) fit their business model.

German companies can establish a market position based on their trustworthiness due to these conditions. Responsible ethical—and thus trustworthy—action is not at all incompatible with economic interests. On the contrary, value-oriented behavior is in the long-term economic interest of providers. In fact, both in Germany and abroad, users are increasingly demanding that AI solutions should be employed in an ethically justifiable manner.

As to the concept of digital sovereignty, it is important to consider this approach holistically for the community of states in Europe and promote it on a fundamental level, thus ensuring that the development and use of AI solutions align with prevailing morals. Moral aspects assume a high priority within the framework of the trustworthiness platform and are expressed through appropriate design, as AI providers must comprehensively state the values on which both their business activities and the design of their AI solutions are based. This enables users to make informed, sovereign decisions about which AI provider and solutions are trustworthy.

References

Absatzwirtschaft: Digitalkonzerne haben Faktor Mensch aus den Augen verloren. https://www.absatzwirtschaft.de/digitalkonzerne-haben-faktor-mensch-aus-den-augen-verloren-vertrauensverlust-von-facebook-google-co-immer-staerker-221217/

Coester, U.: Digitale Ethik—ein Problem in der Marktforschung? In Marktforschung für die Smart Data World. Springer Gabler (2020)

Coester, U., Pohlmann, N: Wie können wir der KI vertrauen?—Mechanismus für gute Ergebnisse, IT & Production—Zeitschrift für erfolgreiche Produktion, Technik-Dokumentations-Verlag (2020) Ausgabe 2020/21

Coester, U., Pohlmann, N.: Vertrauenswürdigkeit schafft Vertrauen—Vertrauen ist der Schlüssel zum Erfolg von IT- und IT-Sicherheitsunternehmen. DuD Datenschutz und Datensicherheit—Recht und Sicherheit in Informationsverarbeitung und Kommunikation, Vieweg Verlag, 2/2022

DENKIMPULS DIGITALE ETHIK: Transparenz und Nachvollziehbarkeit algorithmischer Systeme https://initiatived21.de/uploads/03_Studien-Publikationen/Denkimpulse-Ethik/08-Transparenz-Nachvollziehbarkeit/d21-denkimpuls-ethik08-Transparenz-Nachvollziehbarkeit-Algorithmen.pdf

Luhmann, N.: Vertrauen: Ein Mechanismus der Reduktion sozialer Komplexität, 2000, Lucius & Lucius, Auflage: 4. Auflage, Reihe: UTB: Soziologie fachübergreifend (2000)

Luhmann, N.: „Vertrauen: Ein Mechanismus der Reduktion sozialer Komplexität“, 1968 Luhmann, N.: Vertrauen: Ein Mechanismus der Reduktion sozialer Komplexität. Originalausgabe, F. Enke Verlag, Stuttgart (1968)

Möllering, G.: Forschungsbericht 2006—Max-Planck-Institut für Gesellschaftsforschung. Why do we trust? A theretical approach to an everyday problem

Pohlmann, N.: Cyber-Sicherheit—Das Lehrbuch für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung. Springer-Vieweg Verlag, Wiesbaden (2022)

Suchanek, A.: Ethik und Digitalisierung. In: Hackspiel-Mikosch, E./Neuhaus, R. (Hg.): Ethische Herausforderungen der Digitalisierung und Lösungsansätze der angewandten Wissenschaften (Wissenschaftliche Publikationsreihe der Hochschule Fresenius, Bd. 1), S.21–36, Open-Access-Publikation (2021). ISSN: 2749-4403

Tagesschau: Politiker fordern strengere Regulierung. https://www.tagesschau.de/wirtschaft/unternehmen/socialmedia-facebook-eu-101.html

At the beginning of 2023, Ulla Coester began working as an academic assistant at the Institute for Internet Security, where she is the project leader for the research project 'Trustworthiness Plat-form for AI Solutions and Data Spaces'. In total, she has many years of professional experience, some international, in self-employment as well as in management posi-tions. Until 2022, she was member of the Standardization Evaluation Group in IEC (SEG 10) 'Ethics in Autonomous and Artificial Applications', In 2022, she was con-tributor to the 'Normungsroadmap KI|AG Grundlagen'. Since 2016, Ulla Coester also has been lecturer for 'Digital Ethics' at the Fresenius University of Applied Sciences, Cologne.

Prof. Dr. Norbert Pohlmann is Professor in the Computer Science Department for cyber security and the director of the 'Institute for Internet Security—if(is)' at the Westphalian University of Applied Sciences Gelsenkirchen. He is also chairman of the board of the IT Security Association TeleTrusT and member of the board of the Internet industry association eco.