The Institute of Economics, Zagreb

HrZZ Croatian Science Foundation

Consumer Resilience to Privacy Violation Online

Jelena Budak
Šime Lugović
Zvjezdan Penezić
Edo Rajh
Sunčana Slijepčević
Bruno Škrinjarić

ISBN 978-953-6030-60-6

The Institute of Economics, Zagreb, 2023

PUBLISHER
The Institute of Economics, Zagreb
Trg J. F. Kennedyja 7, Zagreb
http://www.eizg.hr

FOR THE PUBLISHER
Tajana Barbić, Director, The Institute of Economics, Zagreb

EDITOR
Jelena Budak

AUTHORS
Jelena Budak
Šime Lugović
Zvjezdan Penezić
Edo Rajh
Sunčana Slijepčević
Bruno Škrinjarić

PHOTOGRAPHER
Ivona Krezić

PROOFREADERS
Doris Baničević
Tamara Banjeglav
Doris Dresto

TECHNICAL EDITOR
Goran Rožić

GRAPHIC DESIGN
Endem d.o.o.

ISBN 978-953-6030-60-6

This work has been fully supported by the Croatian Science Foundation under the project number IP-2019-04-7886.

Any opinions, findings, conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the Croatian Science Foundation.

Contents

About the REPRICON project

The idea of the REPRICON project was born in late 2018 at the conference "Surveillance, Resilience, & Privacy" held in Paris[1] where a small group of academics and practitioners from various fields and organizations discussed privacy resilience or resilience of privacy and agreed that more research on this topic is needed, both theoretical and empirical, cross-disciplinary and in particular in the social sciences.

Jelena Budak, leader of the project "Extended model of online PRIvacy CONcern (PRICON)" funded by the Croatian Science Foundation[2], made a presentation at the conference which showed that, although not intentionally, PRICON tackled the privacy resilience issue and left open research questions worth further investigation. PRICON findings provided some insights into how Internet users' negative privacy violation experiences are related to privacy concerns and which actions could be envisaged in the case of individuals who have been exposed to privacy breach and those who have not experienced privacy violation. In this respect, the PRICON research model tested the literature-based assumption that negative past experience with privacy violation might raise Internet users' privacy concerns and lead to behavioral consequences: falsification of data, protective actions, and restraining from online activities. PRICON findings only showed that Internet users with prior privacy violation experience expressed higher levels of privacy concern online. Furthermore, PRICON research demonstrated that Internet users tend to trade off online privacy in favor of benefits offered by the Internet. Thus, this tells us nothing about consumer resilience which is a different concept than privacy concern. The PRICON model did not assess the process of recovery after a privacy violation event; instead, it only showed the importance of this process. PRICON did not explore the antecedents and concrete activities in the process of recovery after online privacy violation, opening a new research scope which motivated us to continue exploring this aspect of consumer behavior more in depth.

1 www.surveillanceresilienceprivacy.org/publications/
2 IP-2013-11-7913, www.eizg.hr/publikacije/knjige/the-extended-model-of-online-privacy-concern/3952

When discussing the extension of the PRICON project, we were REvisiting PRICON, REthinking PRICON, witnessing full REvival of the PRICON project, which is why the REPRICON acronym for the new project seemed natural.

In conclusion, the main objective of the PRICON project was to develop and empirically test an integrated model of online privacy concern while the main objective of the REPRICON project is to develop and empirically test the conceptual model of resilience of Internet users who have experienced privacy violation online. It would be logical to assume that Internet users behave according to their experiences and concerns and that bad memories evoke behavior that is more defensive. People who have experienced privacy violations while online might change their intention to adopt new online services or technologies. If an equilibrium after privacy disturbance is not achieved or is established at a lower level of consumer online activity, the implications might be disturbing for business and public policies. Less resilient consumers might decide not to make online purchases or refrain from, for example, e-banking transactions, social networks or even from using smartphones or credit cards.

During the process of developing the project proposal, the team had already learned a lot. First, we understood that resilience is a multifaceted concept explored across diverse academic disciplines and that there is no straight definition and concept of resilience.

At an individual level resilience is conceptualized as the capability of individuals to recover from adversities or as the process of adaptation to adversity. Limited studies of consumer resilience conceptualize resilience at an individual level and explore how consumers recover or adjust their consumption habits after experiencing some form of adversity situation. However, the concept of adaptive responses is not developed here, and antecedents and consumer behavior consequences remain underexplored. This is particularly valid for online context gaining importance in the digital society.

Therefore, the REPRICON project aims to contribute to the privacy resilience debate by exploring how individual behavior is restored after the occurrence of online privacy violation

by theoretically developing and empirically testing the conceptual model of online consumer resilience on the population of Internet users who have, according to their subjective opinion, experienced privacy violation online. The concept of the research proposed a model that will include antecedents of online consumer resilience, identify stressful events experienced as privacy violation, and measure resilience by adaptation responses in terms of concrete online actions undertaken by consumers. Several outcomes are envisaged depending on the adaptive capacity of an individual consumer, whereas adaptive capacity is supposedly formed by antecedents and other determinants such as Internet skills. Responses could be grouped in five behavior outcomes: i) no change in the behavior, indicating resistance to privacy breaches; ii) full recovery, meaning that individuals bounced back to their normal activity as it was before the stressful event happened; iii) partial recovery at the worse-than-before level; iv) recovery at bounce-back-better level in a hypothetical case in which a negative event passed without severe consequences, so the consumer stopped worrying about privacy violation and intensified online activities (thriving); and v) a complete termination of previous activities online that were affected by a privacy violation event. Variations in resilience would be measured by observing how consumer behavior recovers after taking adaptation actions in the course of relative time the process takes. In addition, REPRICON aims to provide answers to the following questions: Do technical security aspects online matter in resilience and consumer behavior? Do personal attributes influence consumer behavior? What individual characteristics shape consumer resilience online and individual adaptation responses? Could Internet users be grouped in clusters sharing the same individual characteristics? What are the implications of consumer behavior and consumer resilience to online privacy violation on digitalization in the public sector? And more generally, what are the implications of consumer behavior for the future of online services and e-economy in the digital society? These questions intrigued our research curiosity and stand at the heart of the REPRICON research project.

We believe this research is the first to develop a theoretical model and empirically test the research model for investigating online consumer resilience, and our work presented in the REPRICON book proves that we have succeeded in this four-year endeavor.

The REPRICON project started in January 2020 and ended in December 2023. Senior researchers at the Institute of Economics, Zagreb form the core research team. Jelena Budak is the principal investigator, due to her previous experience as project leader of the PRICON project. Edo Rajh is a REPRICON team member specialized in marketing research and survey methodology who brought valuable consumer behavior expertise into the project. Together with Edo, Bruno Škrinjarić is another former PRICON team member who joined the REPRICON team as methodology expert in modelling and data analysis. Sunčana Slijepčević brought her experience in studying digitalization in the public sector and implementation of the smart city concept.

Since REPRICON is truly an interdisciplinary project we wanted to include in the project the expertise and synergy effects from colleagues coming from other disciplines and institutions. Zvjezdan Penezić from the Department of Psychology, University of Zadar, contributed, among other things, to the literature review on psychological factors as antecedents and measurement tools used in psychology and in the interviews and focus groups methodology. Šime Lugović, a doctoral student from the Faculty of Economics and Business, University of Zagreb, and an information security expert joined the team and brought his knowledge of digital economy and security.

The project started with an extensive examination of relevant literature in the field, while we parallelly conducted partial studies following the project's work plan. We were aware that the right design of the model and variables, as well as field research that followed, was crucial for the project. Coordinating and monitoring this phase of the REPRICON project required thorough documenting of every step we made, so chapters of the book reflect phases of the project. Although the entire team participated in all phases, some of us were more involved or more familiar with selected activities, so these members appear as authors of associated chapters. The aim of the book is to document our work that might be helpful to other researchers engaged in similar projects. Documenting our activities in this way should help us publish REPRICON project's results in the future as well, if and when we need to recall, for example, details of the methodology applied. During the project, research papers

were produced, submitted for publication or published, and they are included in this book as reprints or in preliminary versions, such as working materials. However, the most important motive for us was to make an extra effort in bringing together our expertise and to produce a publication that will outlive the project. This would be our way of thanking the Croatian Science Foundation for its support to this research.

The REPRICON team much appreciates the assistance of Ivona Krezić, our project coordinator, who took care of all administration connected to the management of such a complex project. Finally, the REPRICON project and this book would not have been possible without the institutional support we received from the Institute of Economics, Zagreb.

About us

The REPRICON team 2020

REPRICON kick-off meeting, January 31, 2020. Photo by Ivona Krezić.

Team members (from left to right)

Bruno Škrinjarić is a research associate at the Institute of Economics, Zagreb. He holds a doctoral degree from the University of Ljubljana and is interested in applied econometrics, economics of education, industrial economics, and consumer privacy concern. His focus within the REPRICON project was on micro-environmental and macro-environmental factors as antecedents, questionnaire development and SEM analysis.

Edo Rajh is a senior research fellow in permanent position at the Institute of Economics, Zagreb, the Department for Innovation, Business Economics and Business Sectors. His primary research areas are market research methodology and measurement scales development. He successfully applied to the REPRICON project expertise in consumer behavior, survey methodology and consumer privacy concern gained from the former PRICON project.

Sunčana Slijepčević is a senior research fellow at the Institute of Economics, Zagreb with specific research experience in public sector economics, regional and urban economy,

multivariate analysis and survey methodology. This expertise helped her assess the consumer resilience to privacy violation and to digitalization in the public sector.

Jelena Budak is a senior research fellow in permanent position at the Institute of Economics, Zagreb. Her research interests include public opinion polls and privacy protection issues, consumer behavior in an online environment, institutions, and the quality of public governance in transition. She was the leader of the PRICON project and led the REPRICON project as well.

Zvjezdan Penezić is a full professor at the Department of Psychology, University of Zadar. His research interests include psychology of personality, personality development, life satisfaction, psychology, and the Internet. Zvjezdan contributed to the REPRICON project by adding the psychological approach to studying consumer behavior online.

Šime Lugović works as an information security expert in a large Croatian bank and is a doctoral student attending a university post-graduate (doctoral) study program in Economics and Global Security at the Faculty of Economics and Business, University of Zagreb. As a member of the REPRICON team interested in digital economy, sharing economy, analytics, and security, Šime contributed to the project with a literature review of resilience engineering and studying the impact of privacy breach on the perceived risk rate in the future.

1. Resilience definitions and concepts[3]

Resilience is a multifaceted and multidisciplinary concept that attracts a great deal of research across numerous and diverse academic disciplines – from ecology, engineering, and computer science (e.g., Brand & Jax, 2007; Klein, Nicholls & Thomalla, 2003; Callister & Rethwisch, 2018; Trivedi, Kim & Ghosh, 2009; Hiller & Russell, 2015), across psychology, medical sciences, and social work (e.g., Herrman, Stewart, Diaz-Granados, Berger, Jackson & Yuen, 2011; Johnson, Gooding, Wood & Tarrier, 2010; Greene, 2002; Wagnild & Young, 1993), to marketing, management, and accounting (e.g., Luthans, 2002; Deans & Garry, 2013; Ollier-Malaterre, 2009; Bhamra, Dani & Burnard, 2011; Ledesma, 2014). The multivariety of meanings of resilience is mirrored in the definition provided by the Oxford English Dictionary: The action or an act of rebounding or springing back; rebound, recoil. Elasticity; the power of resuming an original shape or position after compression, bending, etc. The energy per unit volume absorbed by material when it is subjected to strain; the value of the elastic limit. The quality or fact of being able to recover quickly or easily from, resist being affected by, a misfortune, shock, illness, etc.; robustness; adaptability (Soanes & Stevenson, 2006).

The term resilience originates from the Latin word resilire, meaning to spring back. It was first used in physics and technical sciences to describe the stability of materials and their resistance to external shocks. Specifically, a resilient (or ductile) material can bend when force is applied and return to its original condition once that force is removed. The reversible unfolding of material at the molecular level makes the material more brittle (Campbell, 2008) which explains material resilience close to material elasticity. More precisely, resilience in material science is the ability of a material to absorb energy when it is deformed elastically without creating a permanent distortion.

We have conducted a non-systematic literature review in the field of resilience (Ferrari, 2015; Huelin, Iheanacho, Payne & Sandman, 2015; McDougall, 2015; Snyder, 2019) also called a narrative style literature review (Ferrari, 2015; Green, Johnson & Adams, 2006). The main goal of the method of a non-systematic literature review is to identify a gap in the

3 The following text on concepts and definitions of resilience is based on Budak, Rajh, Slijepčević, and Škrinjarić (2020).

literature, to summarize relevant published research studies, and to define future research directions that have not been previously addressed (Ferrari, 2015). This literature review type is considered vital for papers "devoted specifically to reviewing the literature on a particular topic" (Baumeister & Leary, 1997, p. 311), as well as "a valuable theory-building technique" (Baumeister & Leary, 1997, p. 312). Literature searches were conducted within the Google Scholar and Web of Science databases using relevant keywords related to resilience, its antecedents, and its outcomes. The inclusion criteria referred to the academic papers from various scientific areas, since resilience is a multidisciplinary concept. The exclusion criteria referred to papers not available through the full-text option and not written in English. The summary of types and definitions of resilience is enclosed in Appendix 1.

1.1. Resilience as a holistic concept

Definitions of resilience vary depending on the field of research. Hosseini, Barker and Ramirez-Marquez (2016, p. 47) state that: "The common use of resilience word implies the ability of an entity or system to return to normal condition after the occurrence of an event that disrupts its state." They conclude that currently existing definitions do not contain mechanisms to achieve resilience but conclude that many emphasize the importance of the system to "absorb" and/or "adapt" to disruptive events. In most definitions, "recovery" is a key part of defining "resilience" (Hosseini et al., 2016). Engineering systems, on the other hand, emphasize reliability over "resilience". Bhamra et al. (2011, p. 5376) point out that resilience is a term used in many areas and that the concept of resilience is "closely related to the ability of an element to return to a stable state after a disruption, the condition it was in before the disruption."

The basic concepts associated with resilience are "return to the previous state", "the existence of different sub-states", "shock absorption", and "disruption" itself. These concepts are also often associated with the risk assessment process. Risk management strategies have traditionally focused on reducing the likelihood and potential consequences of the event

in the form of mitigation options, prevention, and protection. Consequentially systems are designed to avoid or absorb undesired events. Many of these terms will repeatedly appear throughout this book because our intent is to explain resilience and related terms and phenomena in various research contexts.

Resilience has become a "boundary object" across disciplines that share the same vocabulary but with different understanding of the precise meaning of resilience. However, as Brand and Jax (2007, p. 9) noted, resilience as a boundary object is "open to interpretation and valuable for various scientific disciplines or social groups, (…) and can be highly useful as a communication tool in order to bridge scientific disciplines and the gap between science and policy". Most of the resilience literature develops resilience theory in their relevant fields but empirical research such as case studies, modelling and in particular surveys which would test the theoretical approaches are rather rare.

Back to the definition of resilience in different contexts and across disciplines, the older definition of resilience refers to the robustness or resistance on the one hand, versus adaptive capacity on the other (Holling, 1973). From these two approaches it is not clear if a resilient system resists adverse conditions, or does it adapt to them. Is the new balance achieved by "bouncing back" (Wildavsky, 1988) or "bouncing forward" to a more desirable state (e.g., Davoudi et al., 2012), and in what timespan would it occur. Manyena (2006) considered resilience as recovery, yet it remains undetermined whether a resilient system resists adverse conditions, adapts to them, or simply can fully recover from damage by bouncing back. Resilience is the broad application of failure-sensitive strategies that reduce the potential for and consequences from erroneous actions, surprising events, unanticipated variability, and complicating factors (Patterson, Woods, Roth, Cook, Wears & Render, 2006).

Resilience is based on the assumption that every system is susceptible to disruptions. How well the system responds depends on its preparedness. In the context of resilience to disasters, Bhamra et al. (2011, p. 5375) criticize disaster preparedness views, as they define "it is often only through hindsight that disasters look like events that individuals should have

prepared for." And indeed, if we look better, after accidents we can often witness different actors condemning the lack of preparation for disaster. The question is how these same actors would react if a huge investment in protection mechanisms against the consequences of a potential disaster were announced, without high probability that a catastrophe will happen.

Ponomarov and Holcomb (2009) identified three elements of resilience: readiness and preparedness, response and adaptation, recovery, or adjustment.

Woods (2017) proposes different views upon resilience, different from viewing resilience as the capacity for adaptation, stating that all systems adapt, but the author negates that resilience is simply the capacity of the system to adapt. Instead, he understands resilience as "how well can a system handle disruptions and variations that fall outside of the base mechanisms/ model for being adaptive as defined in that system" (Woods, 2017, p. 21). He further clarifies resilience as the "ability to recognize and adapt to handle unanticipated perturbations that call int question the mode of competence, and demand a shift of processes, strategies, and coordination." (Woods, 2017, p. 22). He states that resilience is in fact concerned with the boundary condition of the strategies that match demand and how well they expand or adjust current models to react to changing demands.

Longstaff, Koslowski and Geoghegan (2013, pp. 6-7) in their attempt to translate holistic resilience concepts across disciplines describe four resilience types, relating them to different resilience research traditions.

a) Resilience defined as the capacity to rebound and recover is predominantly adopted in traditionally engineered and other designed systems where resilience is seen as a system property or measure of stability.

b) Resilience defined as the capability to maintain a desirable state or to bounce back to an approved equilibrium or assumed normal state is predominantly employed in business, psychology and other social disciplines.

c) Resilience defined as the capacity of the systems to withstand stress where high resilience implies sufficient robustness and buffering capacity against a regime shift and/ or the ability of system components to self-organize and adapt in face of fluctuations.

d) Resilience defined as the capability to adapt and thrive is often conceptualized in social systems and psychology as skill that an individual or group can bring to a disturbance that will allow it to reach a level of functionality that has been determined to be "good." The disciplines in this box acknowledge the existence of multiple possible states, but also explicitly call for a successful adaptation before or after a disturbance occurs. Hence, a positive adjustment can involve different desirable states ranging from a worse, but acceptable level to an even better post-disturbance state. Managing resilience as a normative activity or outcome involves human capabilities such as anticipation, sense-making and learning.

Using the example of social–ecological resilience definitions and concepts of resilience, Strunz (2012) discusses if conceptual vagueness is an asset or a liability in resilience research. Resilience has apparently multiple meanings. Firstly, it denotes how fast the variables return toward their equilibrium following a perturbation. This definition is applicable only to stable systems with one equilibrium. Resilience demonstrated after a system has been disturbed with respect to a specific disturbance is measured ex-post, contrasted to the concept of current resilience in order to predict the consequences of future disturbances.

Arguments in favor of precision prevail in traditional philosophy of science, stressing it is a proven scientific method establishing the validity of concepts and empirical testability. On the other hand, vagueness allows for creativity, interdisciplinary and transdisciplinary approaches that lead to problem-solving. Strunz (2012) argues that a trade-off between vagueness and precision exists, depending on the research context. In some contexts, resilience research benefits from conceptual vagueness while in others it depends on precision. Conclusively, a variety of resilience definitions can exist as long as they are acknowledged.

A rather recent review of resilience is given in Martin-Breen and Anderies (2011, p. 2). Although they consider resilience within the Building Climate Change Resilience Initiative, which framed resilience as "the capacity over time of a system, organization, community or individual to create, alter, and implement multiple adaptive actions in the face of unpredictable climatic changes", their work provides a systematic overview of resilience definitions and concepts that have evolved in ecology and psychology, and increasingly in political sciences, sociology, history, economics and business administration, urban planning, and international development.

In their review paper, Hosseini et al. (2016) identified four domains of resilience: organizational, social, economic, and engineering. While resilience has a clear definition within engineering and psychology it is not the case within the complex adaptive systems research domain or in economics. Several conceptual and review papers have been written to clarify resilience in various fields, for example Klein et al. (2003) review resilience in natural hazards, Brand and Jax (2007) review ecological resilience (or ecosystem resilience) in sustainability science and Norris, Stevens, Pfefferbaum, Wyche and Pfefferbaum (2008) in community resilience .

In the following chapters resilience definitions and concepts are systemized across disciplines as they evolved in theoretical and empirical research. Having in mind the huge research area in which resilience is assessed, it is just a sketch of ample resilience definitions and concepts, and some of them can reappear under multiple titles and categories. However, the ultimate aim is to introduce the concepts that will be borrowed and used in the REPRICON research.

1.2. Ecological resilience

Holling (1973) in his seminal work defined engineering resilience as the ability of a system to return to an equilibrium or steady-state after a disturbance, countering how long it takes for the system to bounce back after a shock. His viewpoint here was to distinguish resilience from stability of ecological systems. In contrast to the engineering resilience measured by the

speed of recovery, about two decades later Holling (1996) defined the ecological resilience as the magnitude of the disturbance the system can take and absorb before it changes its structure, i.e., the system's ability to persist and adapt.

Here, resilience is defined not just according to, but also how much disturbance it can take and remain within critical thresholds. Ecological resilience focuses on "the ability to persist and the ability to adapt" (Adger, 2003, p. 1). For ecologists, resilience is the capacity of an ecosystem to tolerate disturbance without collapsing into a qualitatively different state that is controlled by a different set of processes. A resilient ecosystem can withstand shocks and rebuild itself when necessary. The ecosystem would not look exactly as it was before the disaster because individual species would adapt (Longstaff et al., 2013).

Gallopín (2006) in the context of ecological and socio-ecological resilience developed a model of resilience as a subset element of vulnerability where vulnerability is defined as exposure to external stress, exposure and sensitivity to perturbation and system capacity to response. Resilience together with an adaptive capacity is a subset component of a capacity to response to a stressful event.

Brand and Jax (2007) offer a review of the variety of definitions proposed for resilience within sustainability science and suggest a typology according to the specific degree of normativity. The classification of resilience is made in three main categories: descriptive, normative and hybrid concepts/definitions of resilience. The authors argue that within ecological science a clearly specified, descriptive concept of resilience is critical for operationalization and application of resilience. Their systematization reproduced in Appendix 1 partly refers to the definitions of resilience in social sciences. Distinct to the resilience of ecosystems, Adger (2000) and Adger, Hughes, Folke, Carpenter and Rockström (2005) introduce the resilience of society or communities to stressful events, commonly caused by natural disasters.

1.3. Community resilience and resilience to natural disasters

Resilience is widely seen as a desirable system property in environmental management. Human resilience in disaster planning implies the ability to bounce back and even to grow in the face of threats to (biological) survival (Reich, 2006). A resilient system has to prove key abilities to provide emergency response in the event of crisis. Klein et al. (2003) explore the concept of resilience to natural hazards, using weather-related hazards in coastal megacities as an example. Four typical activities of disaster operations management are mitigation of risks, preparedness for the future response, response in terms of managing the ongoing events during the crisis, and recovery (no matter if it considers bouncing back or moving forward) (Altay & Green, 2006). Despite efforts to build systems that possess resilient capabilities, no system could be completely safe or resilient (Lundberg & Johansson, 2015).

However, due to the research on resilience in human development, planning disaster response and recovery is nowadays much improved compared to five decades ago. Masten and Obradovic (2007) pointed out that resilience theory across the developmental and ecological sciences is rather similar and that findings from the developmental theory and human resilience research are instructive for both individual and community resilience. Adaptive systems are crucial for the resilience of people, including their intelligence, behavior regulation systems, and social interactions with family, peers, school, and community systems. Adaptive systems for human resilience are regulatory systems, personal intelligence and motivation to adapt, macrosystems (such as governments, media), as well as knowledge, memories, and experience of individuals, families, and communities.

In developmental theory, resilience following disaster could take multiple forms, including stress resistance, recovery, and positive transformation. Norris et al. (2008) define community resilience in disasters as a process of adaptation after a disturbance or adversity. Here the community adaptation is valued by population wellness, mental and behavioral health, functioning, and quality of life.

Norris et al. (2008, p. 129) summarized definitions of resilience across socio-ecological literature (Appendix 1).

Conclusively, economic development, social capital, information and communication, and community competence are four pillars of community adaptive capacity. To build collective resilience, communities must reduce risk and resource inequities, engage local people in mitigation, create organizational linkages and social support, which requires flexibility, decision-making skills, and trusted sources of information that function in the face of unknowns (Norris et al., 2008).

1.4. Resilience thinking and system resilience

Resilience thinking represents the conceptual vagueness of the resilience definition and blurred boundaries among concepts used in the research of resilience of (socio) ecological systems. Resilience thinking deals with the dynamics and development of complex social–ecological systems addressing three central aspects: resilience itself, adaptability, and transformability (although there is no clear distinction among them) (Folke et al., 2010).

Systems resilience is maintaining system function in the event of disturbance. It is the appropriate framework to be applied to conditions prevailing in dynamic systems that undergo permanent internal changes. In such systems there is no fixed normal state, only functions of the systems are fixed and known. Therefore, after the disturbance, a resilient system will have its functions restored yet not at the same level or in the same way as it was before the disturbance. Application in the literature is mostly in ecology and developmental psychology, specifically in child development (Martin-Breen & Anderies, 2011).

Haimes (2009, p. 499) defines system resilience as “state of the system (composed of a vector of substates) for which any specific substate may respond differently to different inputs (threats).” Fiksel (2003) tends to explain the resilience and resistance of the system by

using thermodynamics laws. “Each system (ball) has a stable state representing the lowest potential energy at which it maintains order, and each is subject to perturbations that shift it along a trajectory of adjacent states” (Fiksel, 2003, p. 5332). We call this a resistant system. The first system is the so-called “highly controlled system”. As the author states, it can recover “rapidly from small perturbations, but it may not survive a large perturbation” (Fiksel, 2003, p. 5332). The author calls this system resistant. The second system is characteristic for the ecological and social environments, it has multiple adjacent states and is resilient, but it also tends to return to equilibrium. The last system is the most resilient one, basically, it has tolerance for large perturbations, and it shifts to the equilibrium state. For the systems, these new equilibrium states represent a fundamental change to structure or function. Allenby and Fink (2005) claim that there is no such thing as whole system resilience, but one can only define resilience when referencing to the specific system and specific threat. They also propose a definition for resilience: “Resilience is defined as the capability of a system to maintain its functions and structure in the face of internal and external change and to degrade gracefully when it must” (Allenby & Fink, 2005, p. 1034).

Resilience in complex adaptive systems is best defined as the ability to withstand, recover from, and reorganize in response to crises. Adaptability is the key feature of complex adaptive systems which after the disturbance, if resilient, maintain functions but due to the adaptability, not the same structure as it was before the crisis. Complex adaptive systems may also assume new functions, so transformability is often a feature of complex adaptive systems as well.

The resilience concept in systems is mostly developed in the context of ecological and environmental systems. The focus on system properties that emphasizes constant change and reorganization has been a great strength of this resilience concept. Resilience thinking is very valuable in framing and discussing aspects of sustainability and sustainable development. Further, this resilience concept is highly flexible and can be applied to a range of systems across a range of scales from individuals to households, communities, regions, and nations.

In resilience literature vulnerability denotes the opposite of resilience. Gallopín (2006) proposes a diagrammatic summary of conceptual relations among vulnerability, resilience, and adaptive capacity. For the author, there is no crystal clear and simple connection between these terms because as he claims vulnerability in relation to resilience "refers to structural changes in the system, implying changes in its stability landscape" (Gallopín, 2006, p. 301), while resilience "is an internal property of the system, not including exposure to perturbations" (Gallopín, 2006, p. 301). He views resilience as a subset of the capacity of response while the capacity of response is a subset of vulnerability.

Vulnerability and adaptation have been used to refer to individuals. The terms adaptive capacity, transformability, and robustness, on the other hand, traditionally are used to refer to collections of decision-making units (villages, cities, nations, etc.). Likewise, individual vulnerability is the antonym of individual resilience. Resilience means the speed at which a person returns to normal, and sensitivity is the degree of disturbance they are subject to when facing a certain magnitude of crisis.

Hosseini et al. (2016) state that the resilience definition is general and as such, it is applicable in a multidisciplinary field. For Hosseini et al. (2016), existing definitions contain overlaps with already existing terms such as "robustness, fault-tolerance, flexibility, survivability, agility, ...".

Other authors point out that redundancy and robustness are also considered important when designing a system for resilience. Haimes (2009, p. 499) points out that improving redundancy of the system does not directly imply an improvement in overall resilience (for example, redundancy may exist for a single threat but not when assessing vulnerability from another threat), concluding that by improving the system's resilience there are significant advantages in managing the risk.

Various authors call out for more generalizable resilience concepts, stating that robustness and resilience are also conflated often, defining robustness as "the degree to which a system is able to withstand an unexpected internal or external event or change without degradation

in system's performance" (Linkov, Eisenberg, Plourde, Seager, Allen & Kott, 2013, p. 472), whereas resilience is the "system's ability to recover or regenerate its performance after an unexpected impact produces a degradation of its performance"(Linkov et al., 2013, p. 472). Robustness, like resilience, refers to the capacity of a system to continue to function given external shocks but in a short period. Resilience, on the other hand, emphasizes learning and transformation that occur over long periods (Martin-Breen & Anderies, 2011).

All the terms with which the term resilience overlaps do have some points of contact, but resilience is visibly mostly related to what comes after the disruptive event, while robustness, reliability, redundancy and other terms mentioned in the text above refer to, so to say, preparation for disruptive events, that is, to ensure that if they do occur, they do not disrupt the continuity of the system. But how to measure resilience at all? Should one take into account some of the existing terms and concepts such as risk assessment or is resilience completely different in the assessment approach?

Sustainability can also be viewed as a term closely related to resilience, as the systems that are sustainable are also more resilient to the changes relating to their economic, social, and ecological environment. Sustainability is a broader concept than resilience; sustainability is about preservation. Sustainability as a term is often viewed as a burden of fewer resources and more constraints and status quo. It is also often misinterpreted as a goal, rather than a dynamic characteristic of ever-evolving systems. Both resilience and sensitivity are determinants of the engineering resilience of individuals (Martin-Breen & Anderies, 2011). Fiksel (2003) states that as enterprises support worldwide sustainability, they also strengthen their own business sustainability by improving reputation and employee pride. In the end, sustainability can be only achieved by joint ventures, not by the single efforts of a single company.

Adaptation is adjustment in the face of change. It may be positive, negative or neutral. Change may be based on immediate conditions, knowledge of past conditions or new information about predicted conditions. A person, society or species can adapt. Distinctively, coping

is the process of individual intentional change in response to a stressor (Martin-Breen & Anderies, 2011).

Adaptive capacity is closely related to resilience. According to Dalziell and McManus (2004), adaptive capacity is a mechanism for resilience since it reflects the ability of the system to respond to external changes, and to recover from damage. System characteristics that enhance resilience are diversity, efficiency, adaptability, and cohesion (Fiksel, 2003) but it remains unclear how to connect these system characteristics with the characteristics of an individual.

Adaptive capacity and transformability are two aspects of resilience. Adaptive capacity refers to the capability of a particular system to effectively cope with shocks. Increased adaptive capacity would facilitate adaptation to changes, thus increasing resilience.

1.5. Resilience definitions used in REPRICON

In their review of almost a hundred scientific publications on resilience, Bhamra et al. (2011) classify literature on resilience according to the perspectives, topics/concepts and methodologies applied. Among four concepts (behavior and dynamics, capabilities, strategy and performance), most of the studies deal with behavior and dynamics, which is the concept prevailing in the REPRICON research as well. Furthermore, we are interested in the research of resilience from the perspective of individuals (contrasted to the ecological, socio-ecological community, organizational and supply chain resilience). As far as applied methodology is concerned, the most prevalent method is theory building, followed by case study and model development. Survey methodology is rarely employed, and this adds value to the REPRICON research which is based on large survey data.

The REPRICON research explores resilience at the cross section of an individual and psychology, and engineering contexts. We are interested in the capacity of individuals to

rebound from adversity, depending on their individual characteristics. In the specific context of exploring resilience to privacy violation online, it should be considered that resilient individuals possess three common characteristics: an acceptance of reality, a strong belief that life is meaningful and the ability to improvise (Coutu, 2002). We will borrow definitions from organizational and disaster management pointing out the importance of the period of regressive behavior, as well as accounting for previous experiences. The definition of resilience used in REPRICON, therefore, comprehends individual resilience as the capability to recover (fully or partially), to resist and/or adjust to adversity, and to stabilize activity on the new level. In Appendix 1, we present the adapted systematization of resilience types and definitions.

2. Application of resilience concepts

Once the definitions and concepts of resilience have been systemized in different fields of research, in the following chapters we will describe the use of resilience concepts in various practical contexts. There are numerous varieties of resilience research in theory and practice and here we aim to illustrate this by examples of resilience engineering, organizational resilience, and smart city resilience.

2.1. Resilience engineering

The concept of resilience engineering needs to be explained within our research of resilience because it is used and implemented to complex systems facing problems, unexpected disruptions, and unexampled events (Thoma, Scharte, Hiller & Leismann, 2016). Individual subjective notion of privacy violation online is also complex, and a privacy intrusion is a stressful event in which occurrence cannot be predicted in a specific point of time and its scope and consequences are not known in advance. Therefore, both resilience engineering and studying consumers' resilience to privacy violations online apply a holistic approach to similar phenomena.

Resilience engineering is a concept focusing on adaptive capacity to stay in control when facing unforeseen disturbances or events in contrast to the "old" technical concept of safety engineering (Hosseini et al., 2016). Resilience engineering devotes "effort to make observable the organization's model of how it creates safety, in order to see when the model is in need of revision" (Woods, 2017, p. 22). Resilience engineering as described above should raise a red flag when the adaptive capacity needs to be adjusted to meet new forms in the environment that surrounds the model/system.

By managing resilience, one is concerned with understanding the system adaptability, including properties (Woods, 2017).

• Buffering capacity: the size or kinds of disruptions the system can absorb or adapt to without a fundamental breakdown in performance or in the system's structure;

• Flexibility versus stiffness: the system's ability to restructure itself in response to external changes or pressures;

• Margin: how closely or how precarious the system is currently operating relative to one or another kind of performance boundary;

• Tolerance: how a system behaves near a boundary – whether the system gracefully degrades as stress/pressure increase or collapses quickly when pressure exceeds adaptive capacity.

In today's world, threats to complex systems grow exponentially with system complexity. Information security, as the foundation of the security of the digital society, provides various techniques for the protection of information that is exchanged on a daily basis inside and outside the system. Systems theory is based on the relationships between parts that connect them to the whole. Complex systems are also "dynamic, nonlinear, and capable of self-organization" (Fiksel, 2003, p. 5332). Complex systems are subject to a wide range of threats from malicious actors, but also natural disasters. In the following subsections, the concept of information security will be briefly presented together with the basic concepts from the same, such as threats, vulnerabilities, security management through compliance systems. After that, an overview of different definitions of resilience will be given, as well as terms that can often be found as a kind of replacement, but also those that are considered to be building blocks of resilience. Finally, the chapter in resilience engineering that we will see, just like the term resilience itself, is not clearly defined and varies depending on the discipline and field of research.

2.1.1. Information security

Information security is seen as a discipline that includes various dimensions, all of which are steered by the board of directors in companies (von Solms, 2005). The basic CIA triad of information security is something that is a widely accepted standard when referring to the information security consisting of confidentiality, integrity, and availability (ISO/IEC 27002:2005; Bidgoli, 2006; Whitman & Mattord, 2011). Information security is essential in defending critical elements (Whitman & Mattord, 2011) but also in securing information systems of the entity in question. Securing whole governments, states, and nations holding global information that are considered high-value high-risk assets also refers to information assurance (Bidgoli, 2006). Referring to the relevant literature, information security can be seen as a set of control measures to minimize exposure and restricting access to the asset only to the authorized entity to minimize the risk of loss resulted from the exploitation of vulnerabilities by the threat.

Information security should be considered as security for consumers so the information security in some companies can have direct consequences on their business activities. Consumers have come a long way since first adopting the Internet, followed by the adoption of credit and debit cards, and buying with them online that research in the past has dealt with, such as Furnell and Karweni (1999). But even this now 40-year-old research shows that consumers are aware of communication security when buying online (Furnell & Karweni, 1999). Today's consumers are faced with numerous risks relating to the product (Tsiakis, 2012), but they are also "holding" perceived information security defined as "the subjective probability with which consumers believe that their personal information will not be viewed, stored or manipulated during transit or storage by inappropriate parties, in a manner consistent with their confident expectations" (Ab Hamid, 2008, p. 197). Looking at the definition by Chellappa and Pavlou (2002) we can conclude that regulations such as General Data Protection Regulation (GDPR), engage in most valuable inputs that comprise perceived information security, dealing with the security of personal data, information to be

provided where personal data are collected from the data subject (Art. 13 GDPR), etc.

The threat to the system is something that could make the system unstable or make a system come to total failure (Bidgoli, 2006). Although we talk about numerous threats from the outside of the system (Whitman, 2003; Whitman & Mattord, 2011; Jouini, Rabai, & Aissa, 2014) there is also a threat from the inside. This proves that systems need not be defended only from the external source of threat but also from the internal threat (Herrmann, 2007). Internal threats carry a bigger impact which is also harder to control and mitigate (Bidgoli, 2006; Colwill, 2009). These insider threats can range from top management position employees and even board members to some disgruntled employees (Humphreys, 2008). When a threat gets realized and it is no longer "only" a threat but is happening, we consider it an attack (Whitman & Mattord, 2011). Experts tend to make systems that are resilient to attacks, but resilience in some cases means that public key infrastructure (PKI) is so secure that attacks are nearly impossible to carry out (Basin et al., 2016). On the other hand, resilience in network infrastructure is defined as a state, a threshold, that the network has to return to or be in to function normally in operative and service means but it highly depends on the system (Smith et al., 2011). Herrmann (2007, p. 368) defines resilience as "the capability of an (IT) infrastructure, including physical, personnel, IT, and operational security controls, to maintain essential services and protect critical assets while preempting and repelling attacks and minimizing the extent of corruption and compromise." Resilience in the IT and thus in the information system is an exposure of the system to a threat agent à propos how easy it is for the attacker to attack the system or gain access to it (Herrmann, 2007). One could think that resilience could be closely linked to availability, as the more resilient the system is, the higher its percentage of availability (availability is most often shown as a percentage, e.g., 99.99 percent (slang: "four nines") availability means that the system is unavailable only 0.01 percent or 52.60 minutes per year or 4.38 minutes per month).

2.1.2. Risk management and compliance

Application of risk management in information security is used to reduce the possibility of events (i.e., attacks) that could have an impact on the business were they to occur (Blakley, McDermott, & Geer, 2001) or to lower the impact if they do occur (Whitman & Mattord, 2011). When conducting risk identification followed by an assessment, various methodologies exist (Karabacak & Sogukpinar, 2005), but they all comprise of multiple steps, the first of which is the identification of all the risks (threats) that can be identified and current posture of the system, then assessing the possibility of that risk occurring, and lastly, if the possibility is high, prescribing mitigation risk techniques through risk control (Whitman, 2003; Peltier, 2005; Sumner, 2009; Whitman & Mattord, 2011; Herrmann, 2007). These impacts on the system resulting in financial loss (Herrmann, 2007), theft or damage to the information, image, and reputation degradation are measured by severity and estimate of the probability of happening, and thus appropriate steps are undertaken (Humphreys, 2008). Systems not only need to be defended “when in motion” but data at rest need to be secured to attain the three pillars of the CIA triad, i.e., confidentiality of the data is achieved by implementing data classification or by data loss protection methods (Whitman & Mattord, 2011).

When transforming these analyses into measures, there are four directions of action: avoidance of risk, reduction of risk, a transference of risk (risk transfer) and acceptance (Rohmeyer & Bayuk, 2019), some authors adding risk elimination (Pompon, 2016).

Compliance is a steering factor in the field of information security with a whole range of security regulations being prescribed by various institutions. Also, numerous standards are to be met when applying new technologies or if holding a certificate is the aim of the corporation (ISO/IEC 27001:2013; Veiga & Eloff, 2007; Whitman, 2003).

To get certified with standards, organizations must prescribe policies, i.e., for change management so that each technical change is logged/documented and tracked (Pompon,

2016). What is clear is that employees are the key factor in this process, as they are the ones that need to comply with prescribed policies, but how employees perceive policies varies and the companies should be aware of it (Bulgurcu, Cavusoglu, & Benbasat, 2010; Siponen, Mahmood, & Pahnila, 2014).

Audits check whether a company complies with these various policies and assess the levels of protection, but also whether these security policies are enforced the way they should be (Blakely et al., 2001; Whitman & Mattord, 2011). These audits can be external or internal. When audits are internal, it should be essential and a priority for a company to have a separate department that carries out audit of compliance management the way it is done in big companies, i.e., the IT department should not carry out an audit for the IT system. By nurturing this approach, the company assures its compliance on an almost day-to-day basis and thus the system is well-maintained and secured (von Solms, 2005).

After the audit, the well-known last step in the PDCA (plan, do, check, act) cycle is done: acting on identified gaps in the information system to improve security (Humphreys, 2008). High penalties for not complying with the policies also foster thinking about researching the prize and punishment approach in the IS as a method to obtain an even higher degree of compliance in companies (Chen, Ramamurthy, & Wen, 2012).

After analyzing definitions of the term resilience, the authors agreed it was necessary to assess resilience at the level of the whole system, i.e., that it was necessary to make resilience assessments for each subsystem. But is it at all possible to talk about resilience of the system as such or is it necessary to approach the assessments of various related concepts that at first glance constitute the term resilience?

Linkov et al. (2013, p. 472) assert that current methods for improving resilience conflate resilience with risk, stating that resilience is “ability to withstand and recover quickly from unknown and known threats, whereas risk is a likelyhood of “adverse event and the magnitude of the resulting damage.” Haimes (2009) defines multiple terms that are essential to grasp

the concept of resilience, including vulnerability as system state that can be exploited to affect the system, intent as a desire to attack the system, capability as ability to cause some damage to the system and threat as both level of intent and capability. Gallopín (2006) however, discusses different terms such as perturbations and stress, giving definitions for each of them (p. 295):

- Perturbations "are major spikes in pressure beyond the normal range of variability in which the system operates, and commonly originate beyond the system or location in question."

- Stress is "a continuous or slowly increasing pressure (e.g., soil degradation), commonly within the range of normal variability."

The key difference in these two terms is that stress is the component most commonly found within the system, while perturbation is an external factor that acts on the system. When looking at vulnerability, as well as resilience, both depend on the type of threat, but while the system may be resistant to one type of threat, it will not be resilient to another at all (Gallopín, 2006).

Perturbations are also defined by Woods. He states that these perturbations result from the fact that the "model implicit and explicit in the competence envelope is incomplete, limited or wrong" or because "the environment changes so that new demands, pressures, and vulnerabilities arise that undermine the effectiveness of the competence measures in play" (Woods, 2017, p. 22).

When trying to define concepts to improve resilience, authors often conflate resilience and risk (Linkov et al., 2013). Linkov et al. (2013) also point out that robustness and resilience are often conflated. Authors somewhat agree, however, that resilience and vulnerability are two sides of the same coin (Gallopín, 2006), but both terms, when trying to come up with a quantitate approach, should involve measuring vulnerability/resilience of individual

components (Linkov et al., 2013; Haimes, 2009; Gallopín, 2006). Linkov et al. (2013) argue that resilience of systems relies on coordination and communication, and resilience of the entire system should be assessed. When defining resilience and steps for measuring it, Haimes (2009) "flees" from so-called portfolio type of resilience analysis which deals with measuring resilience of the entire system. The author proposes that the only approach to measuring resilience is measuring resilience to specific inputs (threats), pointing out that the system could be resilient to one threat but completely fail to be resilient in the face of different threats. But when tragic events strike one part of the system, it is often inevitable for the other parts to stay intact. Bhamra et al. (2011, p. 5376) pointed out the issue of complexity of the systems and their cascading effect of both good and bad states, as agents in those systems interact with each other.

Hosseini et al. (2016, p. 48) state that the strategy of "collaborative cross-checking is an enhanced resilience strategy in which at least two groups or individuals with different viewpoints investigate the others' activations to evaluate accuracy or validity", which is also really important when trying to assess the level of resilience of the system.

In communication systems, the term for improving resilience is "hardening" the system, that is, improving its defensive capabilities and building multilayered defense by investing money and raising costs. But another way of building a more resilient system is by creating virtual offices, redundant sites, thus improving the experience for the customers and employees, but also creating resilience against many points of attack. Allenby and Fink (2005) define this approach as a portfolio-based approach to minimizing the risk across the social unit as a whole. The authors note that today's modern systems are able to adapt to the unpredictable conditions, "predict, prevent, and gracefully recover from failure" (Allenby & Fink, 2005, p. 1035).

The approach to resilience assessment should be objective and aware of one important fact, and that is that there is no single measure of resilience of the entire system, but it is necessary to:

a) implement the process of assessing resilience of individual subsystems;

b) assess the threats and vulnerabilities of the system itself;

c) calculate residual risk.

Systems can be attacked from various vectors, thus there is no single resilience calculation, but a calculation of multiple resiliencies for a whole range of scenarios. In natural disasters, there is a factor of their unpredictability. An earthquake as a natural disaster cannot be predicted, but the potential magnitude can still be calculated, and thus the system insurance can be set for x times higher value in order to minimize the residual risk.

2.1.3. Assessing risks in resilience engineering

After reviewing the related terms with the term resilience and defining resilience itself, we come to the part that contains an overview of the concepts that can be used in resilience engineering, as well as clarification of the term resilience engineering. We will see how, just as in defining the term itself, there is no common language on how to approach resilience engineering. Some authors even give conflicting definitions of related terms with respect to those we had in previous chapters.

Steen and Aven (2011) propose that resilience engineering represents “an alternative to conventional risk management approaches which are based on hindsight knowledge” (p. 292). They state that risk assessments are based on historical data that could be misleading and that are used for risk calculations. Furthermore, Steen and Aven (2011) define resilience as the “intrinsic ability of a system to adjust its functioning prior to or following changes and disturbances, so that it can sustain operation even after a major mishap or in the presence of continuous stress” (pp. 292–293). They distinguish between two main categories of risk:

• traditional risk perspective that views probability as the main component of risk and interprets probability as “an objective property of the activity being studied” (p. 293);

• alternative risk perspective that views uncertainty as the main component of risk, which uses probability as a “knowledge-based tool for expressing these uncertainties” (p. 293).

After defining the risk perspective, Steen and Aven (2011) carry on to link concepts of resilience, vulnerability (robustness) and risk by first introducing the model of vulnerability:

Vulnerability (robustness) = (C, U|A);

where consequences are denoted as C, U is for uncertainties and A for the occurrence of an initial event. The authors also state that resilience is closely related to the concept of robustness. Authors assert that what separates robustness from resilience is an actual initiating event A. Robustness and vulnerability have fixed A whereas resilience is “open for any type of A”. They define resilience as C, U| any A, including new types of A. It is interesting that in the model, vulnerability robustness can be understood as the interchangeable notion to vulnerability.

In the end, it can be concluded that resilience is essentially a subset of, as the authors call it, “extended risk assessment” given that the list of events in this extended risk assessment (p. 294) is as follows:

• identification of initiating events A;

• cause analysis;

• vulnerability analysis expressing vulnerability (C, P, U, K | A) (P is for probability and K is for background knowledge, assumptions);

- resilience analysis expressing resilience (C, P, U, K | any A, including new types of A);

- risk description and characterization.

Madni and Jackson (2009) state that terms such as safety, reliability, and survivability need to be explained in order to better understand the overlaps between these terms and the term resilience. “Safety is a system property, that encompasses the behavior of and interactions among subsystems software, organizations, and humans” (p. 183). Madni and Jackson (2009) point out that resilience engineering can play a vital role in managing risk factors in modern society because resilience engineering explores insights on failures in complex systems, organizational contributors to risk, and human performance drivers to develop proactive engineering practices. Madni and Jackson (2009) go on to further clarify that there is a need for understanding resilience, how to measure it, and measurements of the production/safety tradeoffs, that in the end leads to a timely update of risk models to enable timely investments in safety.

“Reliability in the engineering domain deals with the ability of the system and its components to perform required functions under stated conditions for a specified period of time” (p. 183). Madni and Jackson (2009) state that resilience offers a different approach by anticipating and planning for the unexpected. We could sum it up by saying that reliability is passive, and resilience is a reactive approach to the uncertainties. The authors continue by saying that “learning is at the heart of resilience engineering in that the changing like-hood of failure can potentially guide proactive changes in making safety-risk tradeoffs without waiting for a mishap to occur” (Madni & Jackson, 2009, p. 184). Moreover, the authors add that “resilience engineering does not assure safe system operation; rather, it does bias the odds in that direction” (Madni & Jackson, 2009, p. 184). Madni and Jackson (2009) propose that resilience engineering requires continuous monitoring of the systems, but that it cannot be engineered by adding procedures, barriers or safeguards.

Hollnagel (2011) states that classical safety efforts are usually focused on unwanted and

unexpected or unpredictable events and discusses how to achieve safety by minimizing or mitigating these events. Resilience engineering sees the "things that go wrong" as a flip side of the "things that go right" and therefore assumes that they are a result of the same underlying process (Hollnagel, 2011, p. xxxiii). Hollnagel (2011) states that resilience engineering basically means understanding the entire system performance, not only when things go wrong, but trying to understand all outcomes. Resilience engineering opposed to the safety efforts recognizes all outcomes (good or bad), whereas safety efforts deal only with negative outcomes. Its downside is also "due to the psychological fact that safety is nearly invisible while a lack of safety is highly visible" (Hollnagel, 2011, p. xxxiv). Hollnagel (2011) carries on by defining resilience as "the intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions" (Hollnagel, 2011, p. xxxvi).

Hollnagel (2011) defines four cornerstones of resilience as:

- knowing what to do or the ability to address actual resilience
- knowing what to look for or monitor, the ability to address critical resilience
- knowing what to expect (threats, disruptions) – the ability to address potential resilience
- knowing what has happened or the ability to learn from experience, the ability to address factual resilience.

By defining these cornerstones, the author proposes that the way to approach engineering resilience is to dive more deeply into each of them and their operative application.

Woods (2017, p. 24) defines that resilience engineering "aims to provide support for the cognitive processes of reframing an organization's model of how safety is created before accidents occur by developing measures and indicators of contributors to resilience such as

the properties of buffers, flexibility, precariousness, and tolerance and patterns of interactions across scales such as responsibility-authority double binds."

2.2. Organizational resilience

Resilience has its application in organizations as well. A resilient organization is one that is still able to achieve its core objectives in the face of adversity (Seville, Brunsdon, Dantas, Le Masurier, Wilkinson & Vargo, 2006) and thrive despite experiencing conditions that are surprising, uncertain, often adverse, and usually unstable (Lengnick-Hall, Beck & Lengnick-Hall, 2011). This means not only reducing the size and frequency of crises (vulnerability), but also improving the ability and speed of the organization to manage crises effectively (adaptive capacity).

The review of organizational resilience literature provided by Duchek (2020) offers definitions used in the research of organizational resilience potential, capacity, resilient companies and similar (see Appendix 1).

Furthermore, Bhamra et al. (2011) elaborated the continuity of organization operations in their literature review of resilience in the context of SMEs emphasizing that no matter the approach applied, "resilience is related to both the individual and organizational responses to turbulence and discontinuity" (p. 5376). Therefore, in all major disciplines dealing with resilience—ecology, metallurgy, individual and organizational psychology, supply chain management, strategic management and safety engineering—resilience is "related with the capability and ability of an element to return to a stable state after a disruption" (Bhamra et al., 2011, p. 5376). One of the specific differences distinguishing individual and organizational reaction is that organizations may develop a business continuity plan (Cerullo & Cerullo, 2004) or contingency and disaster recovery plan, while individuals act in a less organized way to the stressful event.

The early work of employing the concept of resilience in organizations may be illustrated by the study by Hind, Frost and Rowley (1996) who proposed the concept of resilience to identify the cultural factors within organizations as a protective shield against the negative impact of organizational change. Mallak (1998) proposed seven principles for implementing resilience in organizations in order to have individuals who, inter alia, will have positive adaptive responses to situations they face and possess a high tolerance of uncertainty.

Organizations can be less prone to disasters by using a decentralized workforce and also by physical dispersion of assets. Allenby and Fink (2005) point out that these new ways of organizing work culture are not strictly fostered by disasters but are also the result of a globalized economy. Authors oppose the point of view when defining and measuring resilience of the single system, but state that resilience should be a property of the entire system. They state that resilience of the system depends strongly on the effectiveness of cross-domain communication and coordination.

An organization's resilience capacity is developed by strategically managing human resources to create competencies among core employees (Lengnick-Hall et al., 2011). Research of resilience in human organizations emphasizes the ability of organizations to rarely fail and maintain their performance despite encountering unexpected events (Linnenluecke & Griffiths, 2010). Systems, however, operate in complex and uncertain environments which makes them fragile to shocks.

Longstaff et al. (2013) summarize the characteristics of resilient organizations. Those are the organizations which encourage diversity, successfully diversify risks, build knowledge on problem solving, increase options and create opportunities for self-organization, including strengthening local functions, building cross-scale links and networks. A resilient organization (or its specific functions) should possess a set of traits such as experience, intuition, improvisation, expecting the unexpected, examining preconceptions, thinking outside the box, and taking advantage of fortuitous events (Nemeth, 2009). To effectively manage crises, organizations also need to recognize and evolve in response to the complex system within

which the organization operates (situation awareness) and to seek out new opportunities even in times of crisis (Seville et al., 2006).

2.3. Smart city and urban resilience

One of the specific fields where resilience has been applied is urban resilience and the smart city concept. The smart city concept has gained importance in recent years (Bartoli, Hernández-Serrano, Soriano, Dohler, Kountouris & Barthel, 2011). National and local governments across different countries are continuously, to a lesser or greater extent, adopting digital technology in different spheres, from collecting data to providing a diverse range of digital services with the goal of improving the quality of citizens' lives. The need for digitalization is the result of the growing and complex challenges that cities are confronted with, and the concept of smart cities has been developed in response to such a situation (Schaffers, Komninos, Pallot, Trousse, Nilsson & Oliveira, 2011). The concept of a smart city implies the use of digital and telecommunication technologies with the aim of increasing efficiency in the public sector. According to Schaffers et al. (2011, p. 434) the concept of smart cities focuses "on the latest advancements in mobile and pervasive computing, wireless networks, middleware and agent technologies as they become embedded into the physical spaces of cities." Not only national economies, but economies on the global level, have become increasingly connected and dependent on secure flow of data. E-services are becoming a more and more important part of urban development.

The importance of such changes is raised by the fact that by 2050, as many as two-thirds of the population is expected to live in cities (European Commission, 2020). With increasing urbanization, the concerns about governmental and environmental issues are also rising (Ijaz, Ali Shah, Khan, & Ahmed, 2016) and contribute to the necessity of creating smart cities.

Resilience, within the concept of smart cities, can be observed from different angles. The first is urban resilience. The level of urban resilience shows how an urban system, smaller

units within the system (buildings, utilities, transportation networks, enterprises, etc.) and people (different groups of citizens, politicians, planners, etc.) respond to disturbances and critical events (Martin-Breen & Anderies, 2011). Smart cities are part of the transition to digital economy (Dubbeldeman & Ward, 2015). Smart cities collect information and data about citizens, places and activities and use them in urban planning in order to provide services more efficiently and to strengthen resilience in cities (Hiller & Blanke, 2017). Some urban services, such as electricity, water, transportation, etc., are increasingly dependent on technology (Dubbeldeman & Ward, 2015). The urban Internet of Things, as an integration of various technologies and communications solutions (Atzori, Iera & Morabito, 2010), brings benefits to management and optimization of public services by enabling interactions with a wide variety of devices and home appliances (Zanella, Bui, Castellani, Vangelista & Zorzi, 2014).

Resilience is a term used in different contexts, including in urban planning (Martin-Breen & Anderies, 2011). Hiller and Blanke (2017) emphasize that large amounts of private data and information are collected in smart cities and used for various purposes, and it is yet to be determined if privacy can survive. They analyze engineering, ecological and socio-ecological approaches to resilience and apply them to privacy in smart cities.

The other point of view refers to the behavior of citizens as users and customers of public services. The literature indicates that there are many factors which affect whether citizens are willing to use services through advanced ICT, given, among other things, the fact that large databases are then created. Smart cities bring many challenges, especially those related to technological issues, and great attention should be put on security and privacy issues in order to protect citizens' identities and data. Al Nuaimi et al. (2015) summarize the following challenges related to data for smart cities: sources and characteristics, data and information sharing, data quality, security and privacy, costs and population size of cities. To overcome these challenges, they emphasize that it is necessary to raise citizens' awareness about how to safely use ICT solutions for smart cities. If users believe the new system is not secure, they will not accept it for use. People are concerned about privacy online and their behavior

is different depending on the kind and purpose of data collection (e.g., Anić, Budak, Rajh, Recher, Škare & Škrinjarić, 2018; van Zoonen, 2016; Cranor, Reagle & Ackerman, 2000). Therefore, services in the city, within the concept of a smart city, should be adjusted to the characteristics of each user depending on their expectations, preferences, and behavior (Bartoli et al., 2011).

Given that the support and participation of citizens is necessary for the functioning of smart cities, some studies are also dealing with citizens' privacy concerns in smart cities. Van Zoonen (2016) analyzes what kind of privacy concerns could be caused by the use of technology and data collection in smart cities and concludes that privacy concerns in smart cities depend on how people perceive particular data (personal or impersonal) and for which purpose the data are collected (service or surveillance). They differ four areas of privacy concerns ranging from hardly any, in situations when people consider the data impersonal and data are used with the purpose of obtaining a service, to extremely high in situations when people consider data to be personal and used for surveillance purposes.

Many papers are discussing cyber security challenges from different perspectives. Ijaz et al. (2016) in their paper provide an overview of the research dealing with security threats and available solutions for smart cities and notice that security is the weakest link in the implementation of a smart city. However, the use of technology within smart cities brings many benefits. A smart city can bring greater safety, lower costs, better organization, better diagnostics, and personalized treatment (Dubbeldeman & Ward, 2015) and can enable larger participation of citizens in decision-making processes (Rabari & Storper, 2015).

3. Resilience in psychology

In the 1970s, psychologists and psychiatrists first began to pay attention to the phenomenon of "resilience". Resilience was studied primarily in the lives of children, particularly those children who are described as being "at risk" from "psychopathology and problems in development" (Masten, 2001, p. 227).

Within the field of psychology, early inquiry examining resilience represented "a paradigm shift from looking at risk factors that led to psychosocial problems to the identification of strengths of an individual" (Richardson, 2002, p. 309). As already mentioned, resilience is typically defined as the capacity to cope with challenging situations and to bounce back from adversity (Beltman, Mansfield & Price, 2011). Resilience is associated with increased job performance and satisfaction in several professions (Avey, Reichard, Luthans & Mhatre, 2011). It can protect against stress and burnout (Mansfield, Beltman, Price & McConney, 2012) and improves a person's capacity to persist in the long term (Chen & Miller, 2012).

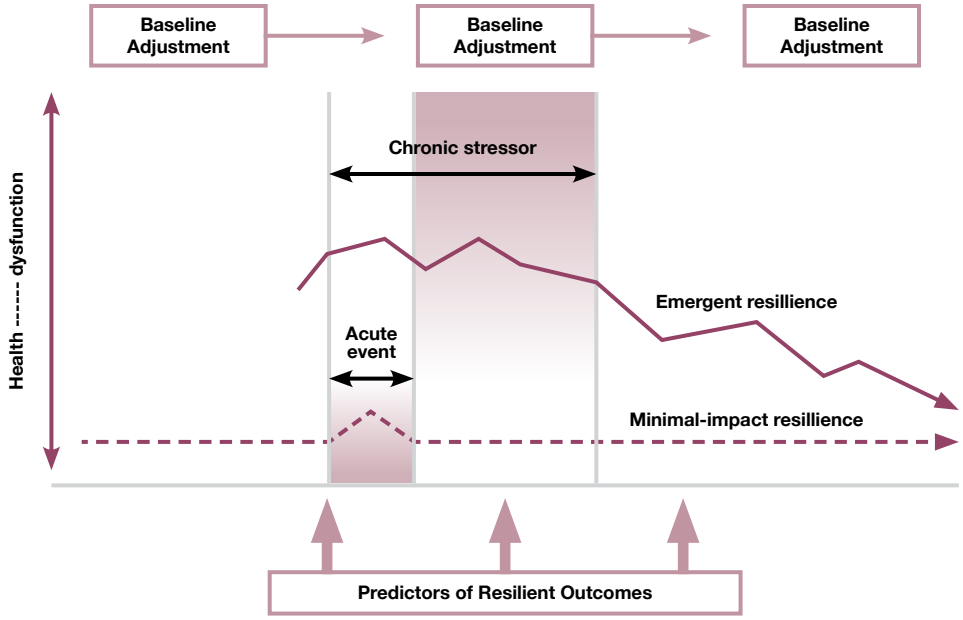
When used in relation to humans, numerous definitions of resilience have been proposed in literature on research in psychology. The specific nature of a definition is often influenced by the historical and sociocultural context within which the research was conducted, the researchers' conceptual proclivities, and the population sampled.

The majority of definitions are based around two core concepts: adversity and positive adaptation. Since the introduction of these concepts to the resilience literature by Luthar and colleagues (Luthar, 2006; Luthar & Cicchetti, 2000; Luthar, Cicchetti & Becker, 2000), they have attracted considerable attention and discussion among scholars (see, e.g., Masten, 2001; Rutter, 2006). Most researchers concur that, for resilience to be demonstrated, both adversity and positive adaptation must be evident. Definitions of resilience used in psychology are presented in the table in Appendix 1.

In accordance with previously mentioned views, Bonanno, Galea, Bucciarelli and Vlahov

(2015) articulate a relatively simple model, consisting of four basic temporal elements, that is broadly applicable across individuals, families, and communities (Figure 3.1). These elements are (a) baseline or preadversity adjustment from which responses to adversity and ultimately resilient outcomes are referenced; (b) the actual aversive circumstances themselves; (c) postadversity resilient outcomes, referenced to both the aversive circumstances and baseline adjustment; and (d) predictors of resilient outcomes measured prior to, during, and after the aversive circumstances.

Figure 3.1. The temporal elements of psychological resilience



Source: Bonanno et al. (2015).

Personal protective factors, which are inherent in the resilient individual by virtue of either biological programming or temperamental attributes, include: innate factors such as autonomy, self-help skills and aptitude, self-efficacy, and impulse control, all geared toward strengthening the individual by buffering risk; familial protective factors (i.e., family factors, including sound family structure and a supportive family network) and extra-familial protective factors (i.e., environmental factors, including bonds with pro-social adults, positive peer relationships, and effective schools).

Davis, Luecken, and Lemery-Chalfant (2009) make a strong collective case for examining the processes underlying positive adaptation in the face of ongoing daily stressors and highly taxing, yet still common, events. Positive adaptation represents adaptation that is substantially better than would be expected given exposure to significant risk. Although indicators of positive adaptation have varied across the context, population, and risk factor under study extant conceptualizations have, in general, included three kinds of phenomena: good developmental outcomes despite high risk, sustained competence under stress, and recovery from trauma (Bonanno et al., 2015; Masten, Best & Garmezy, 1990). On the basis of early reviews of the childhood and adolescence literature, Garmezy (1985) described three major categories of protective factors: individual attributes (e.g., an engaging "easy" temperament and good self-regulation skills), relationships (e.g., parental qualities with high trust, warmth, cohesion, and close relationships with competent adults), and external support systems (e.g., quality neighborhoods and schools and connections to prosocial organizations). These protective factors have been remarkably reliable in predicting positive psychological functioning following adversity (Garmezy, 1987; Masten & Coatsworth, 1998; Rutter, 1987; Werner & Smith, 1992). The consistent support for these assets and resources led Masten (2001) to conclude that resilience emerges not from rare or extraordinary qualities and circumstances but from "the everyday magic of ordinary, normative human resources in the minds, brains, and bodies of children, in their families and relationships, and in their communities" (p. 201).

3.1. Contextual factors of resilience

Davydov, Stewart, Ritchie and Chaudieu (2010) speculated that resilience mechanisms may differ in relation to contextual severity, ranging from resilience against regular everyday hassles like work stress (i.e., mild adversity) to resilience against occasional extensive stress such as bereavement (i.e., strong adversity). Thus, it is important that researchers clearly outline their definition of adversity and provide a reasoned justification for its use.

Ostensibly positive life events can also be relevant in defining resilience. For example, a job promotion, which is unlikely to be labelled as an adversity, will nonetheless necessitate resilience characteristics in positively adapting to the novel demands inherent to the role.

An important, yet often overlooked, issue when examining positive adaptation is the sociocultural context in which an individual operates (Clauss-Ehlers, 2008; Mahoney & Bergman, 2002; Waller, 2001). Ungar (2008) and Ungar and Liebenberg (2011) argued that resilience research has predominantly defined positive adaptation from a Western psychological discourse with an emphasis on individual and relational capacities, such as academic success and healthy relationships.

Mahoney and Bergman (2002) stated that the specific sociocultural conditions in which an individual functions must be considered when examining competence, and that "failing to do so may lead to a view of positive adaptation as a static phenomenon with relevance to only a minority of persons in select circumstances" (p. 212).

3.2. Personal factors and resilience

As mentioned before, resilience involves the capacity, processes, and/or outcomes of successful adaptation in the context of significant threats to functioning or development (Masten et al., 1990). Resilience or "psychological resilience" (Bonanno, Romero & Klein, 2015) is, however, a complex construct that involves traits, outcomes, and processes related to recovery, and has thus been defined differently in the context of individuals, families, organizations, societies, and cultures (Southwick, Bonanno, Masten, Panter-Brick, & Yehuda, 2014).

One such perspective focuses on resilience as personality characteristics that moderate the negative effects of stress and promote adaptation. However, even from this perspective, there have been two approaches—ego resilience (Block & Turula, 1963) and trait resilience

(Connor & Davidson, 2003; Ong, Bergeman, Bisconti & Wallace, 2006; Wagnild & Young, 1993).

The first approach, ego-resilience, is derived from the theoretical model of personality development that was formulated by Block (2002), which centered on two fundamental constructs: ego-control and ego-resilience. Ego-control refers to the individual's characteristic response to behavioral or attentive impulses. Specifically, an undercontroller tends to be highly expressive or attentive to internal pushes and pulls, whereas an overcontroller tends to be constricted in behavioral or attentive impulses, and thus constrained and disciplined (Letzring, Block & Funder, 2005). This dimension reflects different lifestyles and has been indicated to be unrelated to adjustment or competence, as they both tend to be maladaptive.

From the perspective of psychological resilience, researchers have conducted concept-based analyses to elucidate the antecedents, consequences, and essential attributes of resilience (Earvolino-Ramirez, 2007; Windle, 2011). The main antecedent of resilience is deemed to be adversity and the main consequence is positive adaptation. An important debate to emerge from the literature concerns the conceptualization of resilience as either a trait or a process (Windle, 2011). When resilience has been conceived as a trait, it has been suggested that it represents a constellation of characteristics that enable individuals to adapt to the circumstances they encounter (Connor & Davidson, 2003). This notion was first alluded to by Block and Block (1980) who used the term "ego resilience" to describe a set of traits reflecting general resourcefulness, strength of character, and flexibility of functioning in response to varying environmental demands. Individuals with high levels of ego resilience were characterized by high levels of energy, a sense of optimism, curiosity, and the ability to detach and conceptualize problems (Block, 2002). As briefly mentioned earlier, these characteristics have been referred to as protective factors. Since that time, numerous protective factors have been identified in the resilience research literature, including hardiness (Bonanno, 2004), positive emotions (Tugade & Fredrickson, 2004), extraversion (Campbell-Sills, Cohan & Stein, 2006), self-efficacy (Gu & Day, 2007), spirituality (Bogar & Hulse-Killacky, 2006), self-esteem (Kidd & Shahar, 2008), and positive affect (Zautra, Johnson & Davis, 2005).

It could be argued that protective and promotive factors should be considered in relation to their specific function and that an appreciation of the nature and array of these factors is critical to understanding and developing psychological resilience.

While psychological resilience has been conceptualized as a personality trait, it has also been conceived as a process that changes over time. For example, Luthar et al. (2000) referred to it as a "dynamic process encompassing positive adaptation within the context of significant adversity" (p. 543). The process conceptualization of resilience recognizes that the effects of the protective and promotive factors will vary contextually (from situation to situation) and temporally (throughout a situation and across an individual's lifespan). Thus, although an individual may react positively to adversity at one point in their life, it does not mean that the person will react in the same way to stressors at other points in their life (cf. Davydov et al., 2010; Rutter, 2006; Vanderbilt-Adriance & Shaw, 2008). As Rutter (1981) observed, "if circumstances change, resilience alters" (p. 317).

Galli and Vealey (2008) support findings that resilience is a capacity that develops over time in the context of person-environment interactions (Egeland, Carlson & Sroufe, 1993). The interaction between people and their environments is an important consideration when conceptualizing resilience (Waller, 2001). A recent theoretical model that offers a new insight into the role of resilience in the stress process is the meta-model of stress, emotions, and performance (Fletcher & Fletcher, 2005; Fletcher, Hanton & Mellalieu, 2006; Fletcher & Scott, 2010). The basic premise of the model is that stressors arise from the environment an individual operates in, are mediated by the processes of perception, appraisal and coping, and, as a consequence, result in positive or negative responses, feeling states, and outcomes.

It should be taken into consideration that sometimes resilience is related to recovery and that individuals who exhibit resilience seem to be able to proceed with their lives with minimal or no apparent disruptions in their daily functioning. This finding is very important in situations where we can expect some threats, especially in relation to online actions and behaviors. Furthermore, although resilience and coping are often used interchangeably, there is a growing

body of evidence to suggest that these are conceptually distinct constructs (Campbell-Sills et al., 2006; Major, Richards, Cooper, Cozzarelli, & Zubek, 1998; Van Vliet, 2008).

Thus, resilience influences how an event is appraised, whereas coping refers to the strategies employed following the appraisal of a stressful encounter. Another key distinction between resilience and coping relates to the consequences associated with aspects of the stress process (Skinner & Zimmer-Gembeck, 2007; Van Vliet, 2008). Resilience augurs a positive response to a potentially stressful situation (e.g., the experience of positive emotions), whereas the nature of reactionary coping strategies may be positive (e.g., encouraging self-dialogue) or negative (e.g., substance abuse). While individuals who demonstrate resilience are likely to also exhibit effective coping strategies (Major et al., 1998), it is important at this juncture to distinguish between coping "behaviors" and "styles." Resilience is characterized by its influence on one's appraisal prior to emotional and coping responses and by its positive, protective impact, whereas coping is characterized by its response to a stressful encounter and by its varying effectiveness in resolving outstanding issues.

To illustrate, individuals operating in a demanding performance environment daily would be deemed to exhibit resilience if they evaluated stressors as an opportunity for development and, consequently, received peer recognition for their work. In contrast, if individuals operating in a similar environment did not react as positively and their work suffered and, subsequently, they sought social support from their colleagues, this would be an example of coping.

3.3. Personality and resilience

There is considerable evidence that these personality traits can influence psychological resilience among adolescents, as found in earlier studies. For instance, Campbell-Sills et al. (2006) reported that resilience was negatively associated with neuroticism and positively related to extraversion and conscientiousness. In their assessment of some undergraduates' capacity to successfully adapt despite challenging or threatening circumstances, Nakaya,

Oshio and Kaneko (2006) found significant negative correlation between adolescents' resilience and the neuroticism dimension of the Big Five Personality Inventory, and positive values with the extraversion, openness, and conscientiousness dimensions. Similarly, using the Big Five to discriminate between well-adjusted and more vulnerable personality profiles, Annalakshmi (2007) found that all resilience factors were positively correlated with the well-adjusted personality profile obtained. It was also reported that individuals scoring high on resilience scale are psychologically healthier, better adjusted, and thus more resilient (Friborg, Barlaug, Martinssen, Rosenvinge & Hjemdal, 2005).

Bakker, Van der Zee, Lewig and Dollard (2006) reported that a significant relationship existed between burnout and the five basic (Big Five) personality factors: (a) emotional exhaustion is uniquely predicted by emotional stability; (b) depersonalization is predicted by emotional stability, extraversion, and intellect/autonomy; and (c) personal accomplishment is predicted by extraversion and emotional stability.

Considering the range of stresses and traumatic experiences humans can face, the factors that contribute to resilience versus other outcomes including the emergence of psychiatric disorders are important to understand. Understanding these factors can help promote resilience in individuals before they even encounter stress or trauma and can inform the treatment of individuals struggling with stress or trauma. Some of the factors and personality traits are listed below.

3.3.1. Personality traits, optimism, and cognitive flexibility

People with conscientious personalities were found to be organized, thorough, they planned ahead and could control their impulses, which should not be confused with the problems of impulse control found in neuroticism. As reported by Costa and McCrae (1992), people high on neurotic impulsiveness find it difficult to resist temptation or delay gratification while individuals who are low on conscientious self-discipline are unable to motivate themselves

to perform a task that they would like to accomplish. These are conceptually similar but empirically distinct. A considerable amount of research indicates that conscientiousness is one of the best predictors of performance in the workplace and conscientious employees are generally more reliable, more motivated and hardworking (Salgado, 1997).

Agreeableness measures how compatible people are with other people or basically how able they are to get along with others. There is a tendency to be pleasant and accommodating in social situations reflecting individual differences in concern for cooperation and social harmony (Graziano & Eisenberg, 1997). Agreeable traits include being empathetic, considerate, friendly, generous, and helpful and these people also have an optimistic view of human nature. And, as it was mentioned before, optimistic tendency is one of the strongest resilience predictors. Agreeable people tend to believe that most people are honest, decent, and trustworthy and are less likely to suffer from social rejection. Additionally, evidence has shown that, whereas most people are likely to help their own kin or empathize with them, agreeable people are likely to help even when these conditions are not present (Graziano, Habashi, Sheese & Tobin, 2007), thus being traited for helping and do not need any other motivations (Penner, Fritzsche, Craiger & Freifeld, 1995).

Neuroticism has an inherently negative denotation (Bradshaw, 1997), even though (sometimes reversely called emotional stability) it represents an enduring tendency to experience negative emotional states and such feelings as anxiety, anger, guilt, and depressed mood (Matthews & Deary 1998). Goleman (1997) found that people who are high in neuroticism respond more poorly to environmental stress, are more likely to interpret ordinary situations as threatening and minor frustrations as hopelessly difficult. They are often self-conscious and shy, and they may have trouble controlling urges and delaying gratification. Neuroticism is associated with low emotional intelligence, which involves emotional regulation, motivation, and interpersonal skills. It is also a risk factor for “internalizing” mental disorders such as phobia, depression, panic disorder, and other anxiety disorders traditionally called neuroses (Hettema, Neale, Myers, Prescott & Kendler, 2006). Individuals who are high in neuroticism may show more emotional reactions whenever confronted with stressful situations (Van

Heck, 1998). Moreover, they seem to use avoiding and distracting coping strategies, such as denying, wishful thinking, and self-criticism, rather than more approaching strategies (Bolger, 1990; Heppner, Cook, Wright & Johnson, 1995; McCrae & Costa, 1986). Ineffective coping with stressful situations in the work environment makes individuals who are high in neuroticism more vulnerable to the symptoms that are typically associated with burnout (Bakker et al., 2006).

Openness to experience (sometimes called intellect or intellect/imagination) refers to how willing people are to adjust their notions and activities in accordance with new ideas or situations (Goldberg, 1993; McCrae & John, 1992). It includes traits like having wide interests, being imaginative, insightful, attentiveness to feelings, preference for variety, and intellectual curiosity (Costa, & McCrae, 1992). Researchers have demonstrated that people who are highly open to experience tend to be politically liberal and tolerant of diversity (McCrae, 1996; Jost, 2006). There is no relationship between openness and neuroticism or any other measure of psychological well-being. Being open and closed to experience are simply two different ways of relating to the world (Butler, 2000).

Extraversion, also referred to as social adaptability, is the act, state or habit of being predominantly concerned with and obtaining gratification from what is outside the self, defined as “a trait characterized by a keen interest in other people and external events, and venturing forth with confidence into the unknown” (Ewen, 1998). The broad dimension of extraversion encompasses more specific traits such as talkative, energetic, gregarious and assertive.

Optimism comprises primarily cognitive elements. Optimism means maintaining positive expectancies for future events or outcomes (Carver, Scheier & Segerstrom, 2010). Optimism has typically been considered a personality dimension, suggesting it is more of a trait than a state characteristic. Optimism has been associated with self-reported well-being among long-term breast cancer survivors (Carver, Smith, Antoni, Petronis, Weiss & Derhagopian, 2005), psychological adjustment during a life transition (Brissette, Scheier & Carver, 2002),

and reduced PTSD symptom severity after an earthquake (Ahmad et al., 2010). When encountering adversity, maintaining optimism for the future can provide the stamina to endure, but optimism alone is not sufficient to foster resilience.

Cognitive flexibility refers to the ability to reappraise one's perception and experience, instead of being rigid in one's perception. Reappraisal involves finding meaning and positivity in a situation, as well as acknowledging the negative or painful aspects. If one can learn to reframe thoughts about a traumatic event, assimilating these into their memories and beliefs about the event, one may be able to accept and eventually recover. Acceptance and assimilation of a traumatic experience into one's life narrative involves acknowledging that experiences with stress or trauma can provide opportunities for growth, even when there is pain or distress.

Optimism and cognitive flexibility together can enable an individual to maintain faith that they will endure while also accepting the harsh reality they face.

3.3.2. Active coping skills, social support, and physical activity

Active coping skills involve both cognitive and behavioral components. Active rather than passive coping skills are often employed by resilient individuals. The cognitive component includes mindfulness for thoughts about situations and actively minimizing the appraisal of threat to avoid becoming consumed by fear. The behavioral component includes efforts to create positive statements about oneself, facing one's fears instead of avoiding them, and efforts to seek the help and support of others. This is also related to another factor for promoting resilience, maintaining a strong social support network. Close relationships can convey considerable emotional strength to an individual and perceiving an available "safety net" can encourage acting in one's own interest when confronting or recovering from stressful or traumatic situations. The presence of robust social support can influence one's thinking about themselves and their worlds in a positive way. This can help protect against developing hopelessness and other negative psychological outcomes (Panzarella, Alloy, &

Whitehouse, 2006). Taken together, effective social support can engender strength to face fear and trauma and can minimize the experience of hopelessness while encouraging active coping.

Physical activity is primarily a behavioral factor. Attending to one's physical health can help promote resilience. Physical exercise improves physical hardiness and increases strength and stamina, which can increase the chances of survival in traumatic situations.

Physical exercise results in positive effects on mood and self-esteem (Scully, Kremer, Meade, Graham & Dudgeon, 1998), as well as aspects of cognition and brain function (Hillman, Erickson & Kramer, 2008). Maintaining awareness of one's physical hardiness during a traumatic situation can contribute to mental fortitude to endure. Improved mood and increased self-esteem resulting from physical exercise can also facilitate establishing and nurturing social relationships, which are important for promoting resilience.

Finally, it could be noticed that numerous factors are related to resilience and its development. Most of these factors have been measured in relation to everyday situations and there is a need to investigate which factors, of those previously mentioned as well as new ones, are important to resilience in situations when privacy breaches occur.

4. Resilience in social research: Linking consumer behavior and online privacy

The REPRICON research assesses resilience in the social sciences domain. It aims to contribute to the body of knowledge in the social sciences, so a more focused review of the relevant studies is provided below.

Research from the social sciences suggests three core principles of resilience, the "three Cs": control, coherence, and connectedness (Reich, 2006). Raab, Jones and Székely (2015) explore societal resilience to the threats to democracies posed by the current mass surveillance of communications and other applications of surveillance technologies and practices. The authors use an example of public goods to illustrate the distinction between the concepts of resistance and resilience. They describe different outcomes of reactions to shocks in the course of time: resistance prevents deviations from the ideal state, so no recovery is needed, while resilience helps to recover after stress. There are two possible outcomes of resilience: full recovery, which is the return to the previous ideal state, and partial recovery, where the real state after recovery is not equal to the ideal state before the shock. In distinction to resistance which implies invulnerability to stress, resilience implies an ability to recover from negative events (Garmezy, 1991) and the ability of a system to experience some disturbance and still maintain its functions.

4.1. Resilience concept and consumer behavior

Two streams of research are particularly important for our specific context of consumer resilience to online privacy violations. The first stream of research explores the complex inter-relationship between privacy and resilience. Here, resilience is conceptualized at the system-wide level, ranging from an individual information system to the entire social system. Studies within this research stream mainly deal with the question of how to maintain the resilience of the system when its privacy is endangered (Crowcroft, 2015; Hiller & Blanke, 2017). Another

related field of research, with the same system-wide conceptualization of resilience, explores the relationship between surveillance and resilience, and how surveillance (and privacy as its antipode) contributes to or hampers the resilience of societies to various threats (Raab et al., 2015; Jones, Raab, & Székely, 2018).

The second stream of research deals with consumer resilience. Studies within this body of literature, although still rather rare, mainly conceptualize resilience at the individual level and explore how consumers recover or adjust their consumption habits after experiencing some form of adversity situation (Deans & Garry, 2013; Bhattacharyya & Belk, 2019). These studies can be broadly categorized into two groups of approaches (Bourbeau, 2013). The first group explores resilience at the individual level and conceptualizes it as the capability of individuals to recover from or adjust to various adversities and misfortunes or as the process of adaptation to adversity (Bartone, 1989; Cicchetti & Garmezy, 1993; Dyer & McGuinness, 1996; Connor & Davidson, 2003; Visser, 2007; Kotzé & Nel, 2013; Luthar et al., 2000; Luthans, Vogelgesang, & Lester, 2006). The main fields that employ this form of resilience conceptualization are psychology, medical sciences, criminology, social work, and business studies (Olsson, Bond, Burns, Vella-Brodrick, & Sawyer, 2003; Rumgay, 2004; Gilgun, 2005; Gwadz, Clatts, Leonard, Goldsamt, & Lankenau, 2006; Deans & Garry, 2013).

The second group of researchers conceptualize resilience at the broader, system-wide level (Klein et al., 2003; Brand & Jax, 2007; Crowcroft, 2015; Jones et al., 2018). The main fields within this group are ecology, engineering, computer sciences, and political sciences (Nathan, 2016; Lentzos & Rose, 2009; Walker & Cooper, 2011; Omer, Mostashari, & Lindemann, 2014; Sterk, van de Leemput, & Peeters, 2017). In this context, resilience is mainly seen as the capacity of a system to return to its equilibrium state after some disturbance displaced it from its steady state. In computer sciences, resilience is normally present through redundancy, and this approach might be explored in the context of human behavior. Social resilience is defined as a social system's property of avoiding or withstanding disasters, depending on the adaptive capacity of communities or the entire society to prevent future disasters, its coping capacity related to past events, and its participative capacity, denoting the ability of

the social system to change its own structures (Lorenz, 2013).

Literature on consumer behavior is abundant (for a historical overview, see Pachauri, 2001; Solomon, Bamossy, Askegaard, & Hogg, 2013) and more recent studies explore consumer behavior online (e.g., integrated model of e-consumer behavior developed by Dennis, Merrilees, Jayawardhena and Wright (2009) or recent model of online privacy concern by Anić et al. (2018). Consumer behavior studies in the online environment, such as online shopping (Demangeot & Broderick, 2007), e-commerce (Oliveira & Toaldo, 2015), and m-commerce (Sharif, Shao, Xiao, & Saif, 2014) gain importance due to the development of the online marketplace. On the other hand, studies include more specific aspects in the analysis (Dennis et al., 2009), such as online privacy concern (Anić, Škare, & Kursan Milaković, 2019). Research findings show that both privacy concerns and previous privacy violations stand as an obstacle to the growth of e-commerce (Miyazaki & Fernandez, 2001) by inhibiting more customers from engaging in e-commerce (Lee, 2002; Pavlou & Fygenson, 2006; Wang & Emurian, 2005). Although privacy stands as a major concern for online purchasers (Lee, 2002), the skeptical attitude toward online shopping could be mitigated by positive customer experience (Soopramanien, 2011). Balancing between protecting privacy and providing benefits for consumers is a significant challenge for companies because consumers ask for personalized services but resist the collection of personal information (Awad & Krishnan 2006). Privacy paradox and privacy calculus (Smith, Dinev & Xu, 2011) seem to considerably determine the behavior of consumers and need to be addressed carefully in business policies as well. Consumers would voluntarily give away some privacy and disclose personal information in exchange for the benefits of using online services. The benefits an individual gets from using the Internet largely depend on how much insight they are willing to provide about their personal information. The publication of personal data on the Internet occurs consciously (e.g., by self-publishing your profile on social networks, commenting or filling in various forms where personal data are requested) and unconsciously (e.g., by using “cookies” or traces left in search engines or purchases). This disclosure of personal information improves and personalizes services available online for each individual. Furthermore, for-profit business models increasingly rely on the collection of personal information and clients

profiling for client-customized online services (Saurwein, Just, & Latzer, 2015). Taking this into account, it is very difficult and ineffective to completely exclude services that could potentially lead to online privacy violation incidents. Moreover, Acquisti, Brandimarte and Loewenstein (2015) point out that nowadays individuals must constantly balance the benefits of disclosing personal information with the risk of privacy violation. However, although users are increasingly concerned about their online privacy, research reveals the phenomenon of the "privacy paradox", meaning that, despite growing concerns about privacy violations, individuals nevertheless share information that could threaten their privacy, especially on social networks (Norberg, Horne, & Horne, 2007). Enduring privacy violation online might impact their individual privacy calculus and consequently affect the online consumer online (Xu, Luo, Carroll, & Rosson, 2011). Rare studies of consumer resilience indicate that the level of resilience affects consumer attitudes (Rew & Minor, 2018) and purchasing outcomes (Kursan Milaković, 2021) differently, wherein the online privacy violation context has not been regarded.

Recently, Islam (2019) stated that cultural and social factors, demographics (gender, age, education, and income), motivation, perceived risk, trust, and attitude of consumers affect their buying intentions online. However, behavior consequences in the online environment remain under-explored, although they are more complex than those in the offline environment (Ginosar & Ariel, 2017). National and local governments across different countries are continuously adopting digital technology in different spheres, from collecting data to providing different digital services, with the goal of improving the quality of citizens' lives. In this context, citizens' concerns about online privacy and their behavior are different depending on the kind and purpose of data collection (Anić et al., 2018). In addition to that, digitalization raises consumer protection issues for the future development and implementation of e-services in the public sector or the implementation of the smart city concept (van Zoonen, 2016), and requires improved consumer skills, awareness, and individual engagement that would result in sustainable buying decisions (Gazzola, Colombo, Pezzetti, & Nicolescu, 2017). Twenty years ago, back in 1999, consumers were not willing to provide personal information online when asked, and this rate exceeded 95 percent. This rate was highly affected by privacy concerns,

which was, in turn, highly influenced by the skills of consumers (Hoffman, Novak, & Peralta, 1999). As the complexity of protecting the digital consumer rose, the number of movements to simplify and define explicit statements on how consumer data will be used and directives on how to improve consumer skills increased (Mosco, 2017; European Commission, 2011b). Internet skills diminish as the population age increases, and that affects overall consumer activities on the Internet (Hargittai & Dobransky 2017). An important characteristic of digital consumerism is that digital goods are not effective in structuring social relationships, as everyone can have everything (Lehdonvirta, 2012).

4.2. Privacy in an online environment

Thus far, we have delved into the concept of resilience, so now we will switch focus to the other fundamental concept in our research, and that is privacy in general and privacy in an online environment.

The notion of privacy is very individual; it differs from person to person and from one situation to another. Thus, it is not surprising that an abstract term such as privacy is viewed and researched across many different scientific fields and disciplines. The concept of privacy has also been described through its various dimensions, and the approaches may vary depending on the context of studying privacy issues across disciplines.

Among the most cited definitions of general privacy is the one by Alan Westin, who defines it as “claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others” (Westin, 1970). Buchanan, Paine, Joinson and Reips (2007, p. 158) go into more detail and emphasize the different dimensions of the privacy concept: (1) informational privacy refers to the concept of controlling how personal information is collected and used, and it is especially pronounced in the digital age when the Internet made personal information easy to collect, store, process, and use by multiple parties; (2) accessibility privacy overlaps with informational privacy in cases

where “acquisition or attempted acquisition of information involves gaining access to an individual”, but it also extends to cases where physical access is at stake; (3) physical privacy is defined as the degree to which a person is physically accessible to others; (4) expressive privacy “protects a realm for expressing one’s self-identity or personhood through speech or activity”; and (5) social/communicational privacy refers to an individual’s ability and effort to control social contacts. Similarly, Clarke (2009) distinguishes four dimensions of the privacy concept: (1) privacy of the person, concerned with the integrity of the individual’s body, (2) privacy of personal behavior, concerning sexual preferences and habits, political activities, and religious practices, (3) privacy of personal communications, referring to the freedom to communicate without routine monitoring of their communications by third persons; and (4) privacy of personal data, which covers the issue of making the data about individuals automatically available to third parties.

Moving on to a somewhat more recent concept of online privacy, Gellman and Dixon (2011) emphasize the importance of the intertwinement of online and offline privacy issues by noting that what happens offline affects what is done online and vice versa, especially in the age of the fourth industrial revolution when the entire supply chains are becoming predominantly digitized. The Oxford dictionary defines “online” as “controlled by or connected to a computer” and as an activity or service which is “available on or performed using the Internet or other computer network” (Soanes & Stevenson, 2006). Similarly, Gellman and Dixon (2011) define “online” as connections to the Internet in very broad terms, and in its most technical sense it refers to the computers or devices that connect to the Internet and the World Wide Web.

Online privacy has a different dynamic than offline privacy because online activities do not respect traditional national and/or conceptual borders. Online privacy involves the rights of an individual concerning the storing, reusing or provision of personal information to third parties, and displaying of information pertaining to oneself on the Internet. In the digital era, the online privacy concept focuses on personal information shared with family, friends, businesses, and strangers, while at the same time engaging in self-protection of sensitive information (Markos, Labrecque, & Milne, 2012). Before the digital era, securing personal

information and maintaining privacy simply meant safeguarding important documents and financial materials in a safe "material" place, but with the rise of the Internet, an increasing amount of personal information is available online and vulnerable to misuse (Pauxtis 2009; Allen, 2015). Even a simple online activity, such as using search engines, can be potentially misused for consumer profiling. Reed (2014) introduces the term "digital natives" to describe new generations of children who have grown up with the Internet as a presence throughout their entire lives and who are accustomed to these online activities from a very young age. Walther (2011) emphasizes that most people, including these "digital natives", fail to realize that, once uploaded, information stays online more or less forever, and as such can be retrieved or replicated, despite subsequent efforts to remove it.

Finally, it is important to distinguish between privacy and data protection. European Commission (2020) defines data to be classified as personal data for "any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, and also constitute personal data. Personal data that has been de-identified, encrypted or pseudonymized, but can be used to re-identify a person, remains personal data and falls within the scope of the GDPR." Furthermore, under Article 4 of the General Data Protection Regulation (GDPR), personal data is defined as "any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." Flaherty (1989) argues that privacy is a broad and an all-encompassing concept that involves concerns about various forms of intrusive behavior, while, on the other hand, data protection is a subset of privacy that deals solely with the control of the collection, use, and dissemination of personal information. This is also in line with Clark's (2009) privacy dimensions presented above. Currently, data protection is believed to be the most critical component of privacy protection, as more and more aspects of everyday lives are being automated and digitized.

Past research concentrated on privacy issues from many perspectives (as is to be expected given its broad range of applicability), ranging from defining the meaning of privacy, analyzing public opinion trends regarding privacy, evaluating the impact of surveillance technologies, consumers' responses to privacy concerns, causes and different behavior of privacy protection, and the need for balance between government surveillance and individual privacy rights (Kumaraguru & Cranor, 2006; Goold, 2009; Wirtz, Lwin, & Williams, 2007). Previous research has shown differentiated effects on privacy concerns based on various factors, such as culture (Dinev and Hart, 2005; Chiou, 2009; Ur and Wang, 2013), trust in online companies or institutions (Bansal, Zahedi, & Gefen, 2010; Škrinjarić, Budak, & Rajh, 2019) or different demographic characteristics (Wirtz et al., 2007; European Commission, 2011a) and personality traits (Škrinjarić, Budak, & Žokalj, 2018).

In a modern society, privacy is recognized as an individual right and as a social and political value (Raab & Goold, 2011; Solove, 2008; Goold, 2010). With the coming of the fourth industrial revolution, the emergence of technology-based surveillance, a galloping volume of online transactions and the collection and usage of private client data in developing business strategies, both the state and the private sector are holding, processing, and sharing a large amount of personal information. Thus, many governments have put in place privacy protection policies to meet the demands for safety, security, efficiency, and coordination in society. The flip side of the coin is that governments themselves, in the process of securing individual privacy, might gain too much power over individuals, in terms of profiling behavior and purchasing habits. Thus, there is a certain need to balance the privacy of individuals against the legitimate societal need for information (Zureik, 2004). For this need to be positively perceived in the eyes of the public, it must be accomplished in a professional and transparent way. Solove (2008) argues that, in a modern society, the value of privacy must be determined based on its importance to society, and not in terms of individual rights. Goold (2010) argues that citizens would demand a decrease in state surveillance if they perceived it as a threat to their political rights and democracy in general. Several papers have also shown that privacy concerns or previous privacy violations act as a hindrance to the growth of e-commerce (Miyazaki & Fernandez, 2001). Companies have realized that

protecting consumers' private information is an essential component in winning their trust and is a must in facilitating business transactions (Bélanger, Hiller, & Smith, 2002). Wirtz et al. (2007) indicate that citizens who show less concern for Internet privacy are those individuals who perceive that corporations are acting responsibly in terms of their privacy policies, that sufficient legal regulation is in place to protect their privacy and who have greater trust and confidence in these powerholders. However, sometimes, too much information about privacy policies can also have a negative effect on consumers. For example, Ziesak (2013) studies a link between different types of data collection and concerns for online privacy and shows that privacy concerns actually increase when an online seller informs customers about gathering personal and/or behavioral information. Therefore, the attempt to lower privacy concerns by informing users has actually provoked a contrary effect.

Coming back to balancing the need for information with individual privacy concerns and violations – Smith, Dinev, and Xu (2011) explain two interesting concepts: privacy paradox and privacy calculus. The former is a phenomenon where an individual expresses strong privacy concerns but then behaves in a contradictory way, for example, by sharing personal information online. On the other hand, privacy calculus can be explained as a trade-off between privacy concern "costs" and "benefits" in the form of the service obtained. By way of this concept, rational expectations theory states that users are willing to disclose personal information as long as their perceived benefits outweigh the perceived privacy concerns. When weighing potential benefits and losses of disclosing personal information, people think of three types of information privacy benefits: financial rewards, personalization, and social adjustment benefits (Awad & Krishnan, 2006).

Several authors also emphasize that too much individual privacy may be harmful for society and might be used to promote polarization and help reproduce and deepen inequality within society. Etzioni (1999) emphasizes that excess individual privacy can undermine common goods and positive externalities, as it promotes an individual agenda and possessive individualism. Fuchs (2012) argues that we should be more concerned with whose privacy should be protected, rather than how privacy can be protected. His research shows that

the anonymity of wealth and incomes (profits) makes inequalities between the rich and the poor invisible or, at least, less visible, thereby offering no incentives for reducing these gaps. Thus, privacy is posited as undesirable in those cases when it protects the rich from public accountability but as desirable when it tries to protect citizens from corporate surveillance.

Like the concept of privacy, the concept of privacy violations is extremely difficult to define. Increased demand for information and the spread of new technologies that gather personal information indeed limit purely private spaces and increase the number of privacy violation cases. The violation of privacy on the Internet includes an unauthorized collection, disclosure or other use of personal information (Wang, Lee, & Wang, 1998). Solove (2006) identifies four principal groups of "socially recognized privacy violations": (1) information collection, i.e., the way data are gathered – surveillance, interrogation; (2) information processing, i.e., storing, analysis and manipulation of data – aggregation, identification, insecurity, secondary use of information, and exclusion; (3) information dissemination – breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation of someone's identity, defamation before the public in false light; and (4) invasions – intrusion into someone's private sphere and decisional interference, which is connected to information privacy. However, perceptions of privacy violations can be very subjective. An individual who had a bad experience of online privacy violation might be more privacy concerned (Afolabi, Ozturen, & Ilkan, 2021; Xu et al., 2011) and, likewise, depending on the seriousness of privacy breach consequences, their recovery could be harder (Bansal & Zahedi, 2015; Calo, 2011).

Online privacy violations became a real threat that should be addressed by both the government (Chang, Wong, Libaque-Saenz, & Lee, 2018) and businesses (Beke, Eggers, & Verhoef, 2018) in order to increase the trust of consumers and to size down the perceived risk (van Schaik, Jansen, Onibokun, Camp, & Kusev, 2018). Privacy theft can be carried out on systems that are easily fooled by spoofing (Wolfond, 2017) and these thefts have a large impact on the consumers' feeling of security. There is also an enormous impact if the financial position of a consumer is affected by a privacy theft, such as online payment, without the consumer's consent. These situations occur because traditional systems (e.g.,

banking) require a consumer to be authorized using only their own information, such as a username and a password (Cai & Zhu, 2016), but new technologies, such as Artificial Intelligence (AI), can be leveraged to secure the consumers' positions on the market, as well as their identity (Contissa et al., 2018).

Since the offset of the fourth industrial revolution, information privacy has been in the focus of e-commerce and marketing strategies toward consumers when the government and different online companies want to collect consumer information (oftentimes, not allowing them to proceed with their purchase without providing some sensitive personal information), and consumers often view this practice as a privacy violation. Information privacy concerns and violations present a significant obstacle to more people engaging in e-commerce (Wang & Emurian, 2005; Pavlou, & Fygenson, 2006).

In response to previous privacy violation experiences or as a means of preventing privacy violations, individuals adopt different strategies to make them more secure online. Gurung and Jain (2009) list the suggested typologies of individuals regarding their online privacy violations: (1) privacy aware, referring to being knowledgeable and sensitive about risks associated with sharing personal information online; (2) privacy active, referring to active behaviors adopted by consumers in regard to their privacy violation concerns; and (3) privacy suspicious, referring to concerns about particular company's or individual's behavior regarding their privacy practices. In terms of protection against privacy violation, Yao (2011) and Gurung and Jain (2009) posit that, from an individual perspective, it can be either passive or active. Passive protection involves relying on a government or other external entities, and it is beyond the direct control of an individual. The level of such protection is also dependent on collective actions and institutional support, as well as on cultural and socio-political norms. On the other hand, active protection relies on individuals themselves actively adopting various protective strategies. Examples of these strategies may include abstaining from purchasing, falsifying information online, and adjusting security and privacy settings in web browsers (Chen & Rea, 2004).

4.3. Consumer online behavior in the European digital agenda[5]

The new EU Cohesion Policy 2021-2027 highlighted the objectives within the EU digital agenda. The development of Information and Communication Technologies (ICT) is considered vital for Europe's competitiveness in today's increasingly digital global economy[6] and contributes to reducing economic and social inequalities between EU regions and its periphery. The cohesion policy aims to "make Europe fit for the digital age[7]" through a set of coordinated objectives and policies enabling smooth digital transformation. The objectives of "going digital", "smart specialization", "cohesion", and other buzzword-like processes are supported by immense EU funding: about EUR 500 billion will be available for the EU Cohesion Policy 2021-2027, out of which the allocated EU funds will amount to EUR 392 billion[8].

One of the components of this multifaceted and complex process of EU cohesion is the increased availability and usage of online activities. Strengthening e-commerce, e-government, e-learning, e-inclusion, e-culture, and e-health are at the core of the EU Cohesion Policy digital action plans, leading to a more competitive and smarter Europe. Building the infrastructure would allow access to online services and, in combination with advanced ICT skills, these improved capacities would reduce the digital divide gap. This is, in turn, expected in order to lower the inequalities among European regions. Goals set on the macro-policy level depend on individual actions, attitudes, and behavior on the micro-level. In time of pandemics, consumers turn to online shopping, e-banking, e-learning, e-government services, and other online services even more, for the sake of convenience, accessibility, and safety (Das et al., 2021). This increase in the volume of online activities also carries certain privacy risks with it and raises privacy concerns (Anić et al., 2019; Baek, Kim & Bae, 2014; Bansal & Zahedi, 2015; Ginosar & Ariel, 2017; Liao, Lu & Chen, 2011; Škrinjarić et al., 2019).

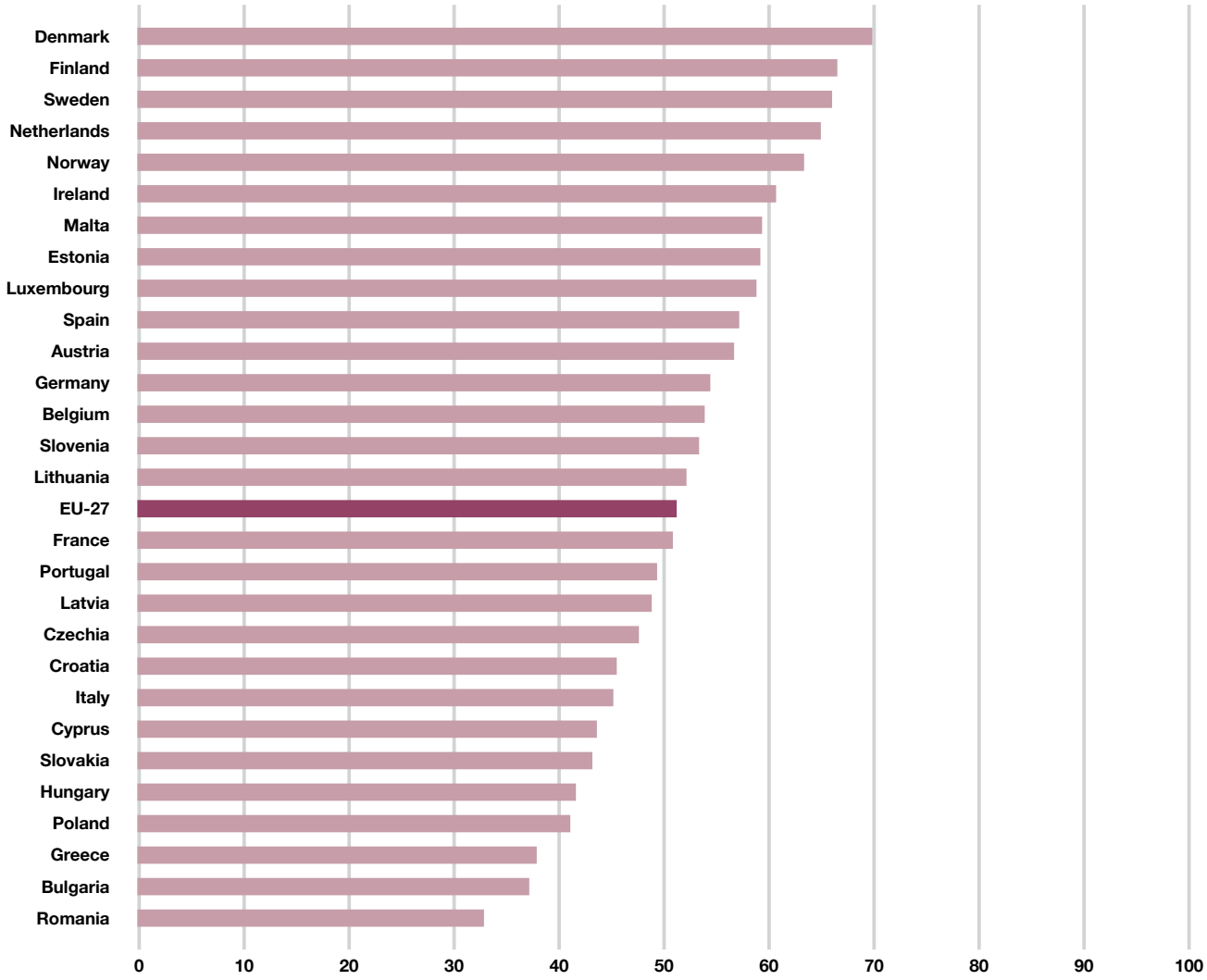
5 This work has been presented at the 9th REDETE2022 conference in Ancona, 15–16 September 2022, and it has been published in the conference proceedings as Budak and Rajh (2022).
6 www.ec.europa.eu/regional_policy/en/2021_2027/
7 www.ec.europa.eu/regional_policy/en/policy/how/priorities/digital-age
8 www.ec.europa.eu/regional_policy/en/funding/available-budget/

Although consumer online attitudes and behavior in European countries are important for fostering the adoption of e-services, relevant research is rare. Androniceanu, Kinnunen, Georgescu, and Androniceanu (2020) explored the behavior of EU consumers in the online environment by considering consumers' individual attributes and habits. Their results indicated five clusters of consumers differing in socio-demographic and e-buying characteristics. For EU-27 countries, Bădîrcea, Manta, Florea, Popescu, Manta, and Puiu (2021) found that socio-demographic factors, such as education, residence, employment status as well as some Internet services usage (e.g., e-banking) affect the development of e-commerce. Past studies are not conclusive about the impact of gender (Akman & Rehan, 2014) and age (Hwang, Jung, & Salvendy, 2006) on e-commerce. However, none of these studies considered privacy concerns and security incidents online when explaining e-commerce activities practiced by consumers.

There are more studies on individuals and e-commerce at the individual country level. For instance, e-commerce penetration in Spain was studied by Valarezo, López, and Pérez Amaral (2020), online privacy concern impact on e-commerce in Croatia by Anić et al. (2019) and Wiktor, Dado, and Simberova (2021) analyzed e-commerce development in Czechia, Poland, and Slovakia in the light of the EU Single Digital Market Strategy. The scope of such studies varies, so findings are not comparable and do not lead to common conclusions.

Digitalization offers benefits for individuals (Elmassah & Hassanein, 2022), companies (Parviainen, Tihinen, Kääriäinen, & Teppola, 2017; Rosin, Proksch, Stubner, & Pinkwart, 2020), and governments (Terlizzi, 2021). In their analysis of countries worldwide, Sabbagh et al. (2012) found that digitalization has a positive impact on economic progress, social well-being, and government effectiveness. Dobrolyubova, Klochkova, and Alexandrov (2019) argue that government digitalization increases public administration performance, which, in turn, has positive outcomes for citizens and businesses. However, recent studies point out there are negative implications of digital transformation for individuals, organizations, and society (Trittin-Ulbrich, Scherer, Munro, & Whelan, 2021) as well. Elmassah and Hassanein (2022) found that, in some segments, digital transformation negatively affects the life satisfaction of EU citizens.

Figure 4.1. Digital Economy and Society Index, 2021



Source: European Commission,

www.digital-strategy.ec.europa.eu/en/policies/countries-digitisation-performance

The level of digitalization is relatively hard to measure precisely because of the complexity of transformation. The methodology of assessing the levels and trends in digitalization has been developed and applied to EU countries in the form of the Digital Economy and Society Index (DESI). DESI is a composite index published annually by the European Commission since 2014. It measures the progress made by the EU Member States toward a digital economy and society, combining a set of relevant indicators. DESI is composed of five principal policy areas, which group 37 indicators overall, and ranges from 0 to 100. The latest DESI available

for 2021 ranks Scandinavian countries as the most digitalized economies and societies in the EU-27 (Figure 4.1). Similar attempts of applying DESI methodology to countries worldwide showed that countries with a higher GDP have a high level of digitalization of public services and a medium level of digitalization of the business environment. Less developed countries are lagging in digitalization and are still focusing on building the infrastructure and ICT skills needed for the upper level of digital transformation (Volkova, Kuzmuk, Oliinyk, Klymenko, & Dankanych, 2021).

One of the issues connected with digitalization is the privacy and data protection nexus. Seemingly, the relation is two-fold: the digitalization process requires giving up some privacy for the benefit of e-services, and privacy behaviors are affected by the adoption of digitalization. The adoption of digitalization might face privacy-related obstacles (Linsner, Kuntke, Steinbrink, Franken, & Reuter, 2021).

Economic theory assumes that individual actions are rational. People tend to provide personal information voluntarily in exchange for benefits but will keep information undisclosed if they see no benefits in return. The trade-off between privacy concerns “costs” and “benefits” is called the privacy calculus. Given the widespread Internet usage, the two intertwined concepts of privacy paradox and privacy calculus drew attention in the marketing and information privacy literature (Smith, Dinev, & Xu, 2011). A privacy paradox is described as a dichotomy between privacy attitudes and privacy behavior, where an individual expresses strong privacy concerns and behaves in a contradictory way.

Empirical evidence produced different results because some studies confirmed the inconsistency and other studies did not prove the existence of the privacy paradox (Kokolakis, 2017; Gerber, Gerber, & Volkamer, 2018). More recent studies indicate that the gap between privacy attitudes and behavior might diminish due to overall digitalization (Dienlin & Trepte, 2015).

The privacy paradox is important for exploring consumer behavior online. If a consumer

neglects their privacy concerns because the estimated benefits of using the Internet surpass the potential losses caused by disclosing private information, they would use the Internet and e-services to the same extent or more intensively as a non-concerned consumer. Otherwise, more privacy-concerned consumers would refrain from e-transactions. Further, there is a reason to believe that the result of the privacy calculus and the existence of the privacy paradox depends, among others, on how resilient a person is to privacy violations online (Budak, Rajh, Slijepčević, & Škrinjarić, 2021).

Heightened protective behavior resulting in fewer e-activities represents an issue for organizations (Gotsch & Schögel, 2023) and nations fostering an e-economy. The individual trade-off decision is a consequence of the privacy calculus, so on one side, effective policies should aim to decrease privacy violation costs and on the other side, to increase the benefits of online services. Scattered research on the privacy paradox did not reach a consensus, so more studies of its causes and consequences in a comprehensive theoretical model are needed (Kokolakis, 2017). If there is a privacy paradox confirmed in the online behavior of Internet users in European countries, the privacy concern might not be seen as an obstacle to the increased usage of digital services, such as e-commerce, e-government, and other objectives on the EU digital agenda. If it proves the contrary, privacy and security issues might deter citizens from “going online”, at least for some specific online activities. If certain activity on the Internet is perceived as a security or privacy risk, an individual might refrain or withdraw from using it, notwithstanding their (increased) availability. Therefore, the following analysis of online consumer behavior in European countries includes concerns and privacy and security incidents experienced online.

The analysis is performed using the Eurostat secondary data for the latest available year (2021 or, exceptionally, 2020) for 38 European countries.

The population in focus are frequent Internet users, represented by the percentage of individuals using the Internet on a daily basis (I_DAY) and online consumers (I_ECOM). Next, we were interested in including Internet users who undertake personal data protection

activities in the analysis, such as reading privacy policy statements before providing personal data, restricting, or refusing access to the geographical location, limiting access to profiles or content on social networking sites or shared online storage, not allowing the use of personal data for advertising purposes, or checking that the website where personal data was provided was secure. Privacy and protection of personal data are expressed by the percentage of individuals who recently managed access to personal data on the Internet (I_MAPS). Despite controlling for privacy and protection of personal data, Internet users experienced privacy violations and security incidents, such as fraudulent credit or debit card use when using the Internet, online identity theft (somebody stealing the individuals' personal data and impersonating individuals, e.g., shopping under an individual's name), receiving fraudulent messages ("phishing") when using the Internet, being redirected to fake websites asking for personal information ("pharming") when using the Internet, experiencing the misuse of personal information available on the Internet resulting in, e.g., discrimination, harassment, bullying, having their social network or e-mail account hacked and content posted or sent without the individuals' knowledge, and experiencing the loss of documents, pictures or other data due to a virus or other computer infection (e.g., worm or Trojan horse). This part of the population of Internet users is expressed by the variable I_SECANY. Finally, to assess the privacy concern as a perceived obstacle to online purchases, we accounted for individuals whose reason for not buying online was having concerns about payment security or privacy (I_NBPSC1).

The progress achieved in digitalization is expressed by the DESI index. To distinguish European countries according to institutional set-up and EU status, we assigned a dummy variable 1 to "old"-EU members and more developed European countries, and 2 to new-EU member states, candidate countries, and other non-EU members. Variables definitions and sources are presented in Table 4.1.

Table 4.1. Variables and definitions

Variable	Description	Source
I_IDAY	Percentage of individuals using the Internet daily	Eurostat ISOC_CI_IFP_FU Individuals – frequency of Internet use
I_MAPS	Percentage of individuals who manage access to personal data on the Internet in the last 3 months	Eurostat ISOC_CISCI_PRV20 Privacy and protection of personal data
I_ECOM	Percentage of individuals using the Internet for e-commerce activities	Eurostat isoc_bde15cbc E-banking and e-commerce
I_NBPSC1	Percentage of individuals whose reason for not buying via a website or an app in the last 3 months was having concerns about payment security or privacy	Eurostat ISOC_EC_INB21 Internet purchases – perceived barriers
I_SECANY	Percentage of individuals who experienced a security-related incident	Eurostat ISOC_CISCI_PB Security-related problems experienced when using the Internet
DESI	The Digital Economy and Society Index measures the progress made by the EU Member States toward a digital economy and society. The score ranges from 0 to 100.	European Commission country reports www.digital-strategy.ec.europa.eu/en/policies/countries-digitisation-performance
EU Status	Dummy variable denoting EU status. Score 1 denotes old-EU members, Norway, Switzerland, and Iceland; score 2 denotes new EU member states, candidate countries, and other non-EU members	European Union country profiles www.european-union.europa.eu/principles-countries-history/country-profiles_en
European countries (n=38)	Albania, Austria, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Kosovo, Latvia, Lithuania, Luxembourg, Malta, Montenegro, Netherlands, North Macedonia, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, United Kingdom	

Source: Authors.

The data were analyzed by means of K-means cluster analysis to identify the groups of countries with similar profiles based on the I_DAY, I_MAPS, I_ECOM, I_SECANY, and I_NBPSC1 variables. ANOVA and chi-square test were used to examine the differences between the identified clusters for EU status and DESI variable.

The K-means cluster analysis was applied to classify the European countries according to the I_DAY, I_MAPS, I_ECOM, I_SECANY, and I_NBPSC1 variables. The Hartigan index was used as a criterion for determining the number of clusters in a data set. Values for the analyzed variables for each country were taken as an input in the K-means cluster analysis. The K-means cluster analysis identified two homogeneous clusters of European countries. ANOVA results indicated that there are statistically significant differences among those two identified clusters for four out of five analyzed variables (I_DAY, I_MAPS, I_ECOM, I_SECANY). There are no statistically significant differences for the I_NBPSC1 variable (Table 4.2).

Table 4.2. Results of the K-means cluster analysis

Variables	Cluster 1 n=19	Cluster 2 n=12	ANOVA
I_IDAY	92.5	82.2	F=37.74; p=0.00
I_MAPS	75.4	56.8	F=31.14; p=0.00
I-ECOM	71.3	38.9	F=55.95; p=0.00
I_SECANY	37.7	13.1	F=39.73; p=0.00
I_NBPSC1	6.0	6.9	F=0.17; p=0.68

Source: Authors.

The first group of countries (Cluster 1) has higher values for the I_DAY, I_MAPS, I_ECOM, and I_SECANY variables when compared with the second group of countries (Cluster 2). Despite the observed differences between these groups of countries, both groups of countries have the same average level of the I_NBPSC1 variable.

Table 4.3. Differences in DESI and EU status among clusters, ANOVA, and chi-square test results

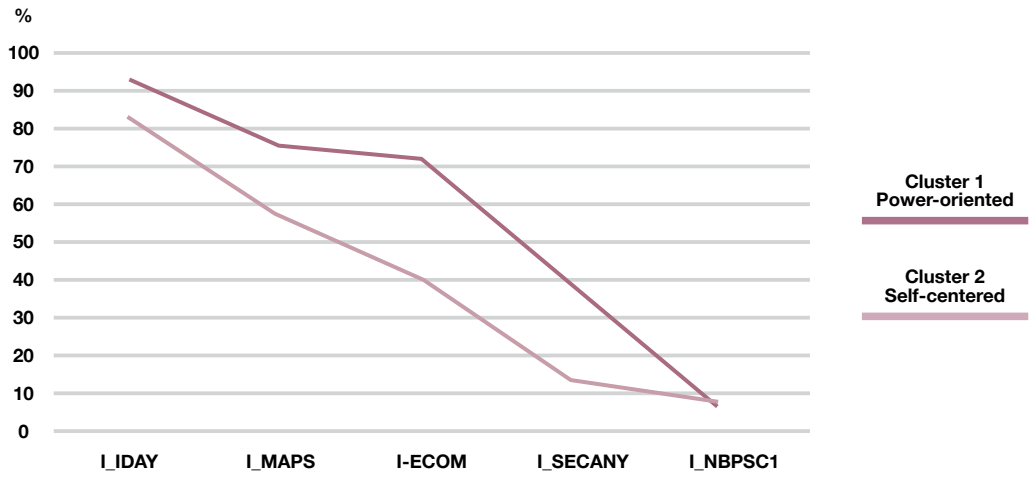
Variables	Cluster 1 Means	Cluster 2 Means	ANOVA
DESI	57.3	44.9	F=14.30; p=0.00
	%		Chi-square test
EU Status 1	73.7	16.7	Chi-square: 9.57; p=0.00
EU Status 2	26.3	83.3	

Source: Authors.

The ANOVA and chi-square tests were also conducted to further explore the differences among the identified clusters. The test results indicated that there are statistically significant differences among the identified clusters, both in terms of DESI variable values and the countries' EU status (Table 4.3).

The cluster analysis results (Figure 4.2) generated interesting observations to be further discussed.

Figure 4.2. Cluster analysis results



Source: Authors.

Both clusters are composed of "heavy" Internet users because more than 80 percent use the Internet every day (I_DAY). However, there are differences in how they manage to control

access to their personal data on the Internet (I_MAPS). Cluster 1 takes slightly better care of restricting and controlling access to its information online. In comparison to Cluster 2, these are Internet users who perform more e-commerce activities, although they had experienced some form of violation of online privacy or security transactions on the Internet. Both clusters have the same low score in giving up Internet shopping for the reason of privacy concerns and the security of online payments.

The main characteristic of Cluster 1 members' attitudes and behavior is that, despite the privacy and security incident experienced, they do not refrain from e-commerce, and manage access to their personal data online. Cluster 1 members are predominantly more developed EU-member states, with advanced digital economies and societies.

Cluster 2 members control the access to their personal data online less successfully, perhaps because they are less concerned and have less experience with payment security put on risk, as well as privacy online violation incidents. The fact that they had rarely been victims of privacy violations and security payment incidents might increase their trust in the safety and security of online transactions. Therefore, members of Cluster 2 continue to use e-commerce; however, to a lesser extent when compared to Cluster 1. The general level of digitalization of Cluster 2 member states is lower when compared to Cluster 1. It mostly consists of new and non-EU countries.

It seems that privacy concerns did not prevent most consumers from shopping online, so at least when it comes to e-commerce activities, the privacy paradox in the EU countries is confirmed. It suggests that, despite potential privacy concerns, Internet users are willing to give up some privacy for the benefits of using e-services. Therefore, privacy concerns of the majority Internet population in European countries should not be seen as an obstacle to further digitalization. However, there seems to be about 6 to 7 percent of the surveyed population refraining from e-commerce because of privacy and security reasons. The successful digitalization process should take into consideration this share of European citizens worth involving in e-services (and e-buying).

The most important finding is that there is a part of the Internet population in all observed countries that will not engage in e-buying because of privacy and online payment security concerns. This share of Internet users is the same regardless of the experienced privacy violation and reflects the attitude toward e-commerce. Withdrawal from this type of online activity might be caused by bad experiences (one's own or those of people close to them), information from the media, personal characteristics of an individual, etc. The cluster analysis does not allow us to draw conclusions about causal relations, and more importantly, to match the attitudes, experiences, and behavior of one individual respondent.

Since both clusters have similar shares of citizens engaged in withdrawal from online buying due to privacy and security concerns, policy recommendation might be to employ various educational measures and technology policies to reduce such shares by introducing alternative strategies of dealing with privacy and security concerns. Instead of withdrawing from online activity, the possible alternative strategy might be engaging in protective behavior, which could decrease the risks of privacy and security incidents but still allow consumers to participate in e-commerce activities.

Once we know how Internet usage and e-commerce activities are related to personal data management applied on the Internet and experienced online security incidents, and that specific groups of Internet users might sustain from e-buying activities for privacy and security reasons, further insights should be achieved by collecting primary data on the individual level of consumers. The conceptual research model for that purpose is described in the next chapter.

4.4. Privacy violation incidents

This chapter introduces various forms of threats to which individuals are potentially exposed in different situations, describes a potential model of attack phases, and an assessment of potential risk. With the rapid proliferation of online technologies on computers and, more recently, mobile devices, the protection of personal information and behavioral data has become an important issue in today's networked society (Acquisti et al., 2015). The notion of privacy in the digital world is essentially no different from privacy in the "offline" world. Personal data are information that can be associated with an individual and thus identify them. In the analog world, personal data are in the possession of the person to whom they relate to (appearance of the person, identity card, fingerprint), and if the person needs to be identified, the personal data are currently available for consultation (identity card, etc.). In this way, a certain level of privacy is relatively easy to achieve.

A privacy impact assessment (PIA) is the process of identifying and mitigating privacy risks in an existing or planned system. During a privacy impact assessment, organizations identify potential privacy risks, quantify and evaluate those risks, and, finally, make decisions about whether and how to mitigate, eliminate, transfer, or accept the risks. PIA also refers to the document created in this process and is generally considered a living document in system development. This is because privacy risks can change over time: as a result of decisions made during design and implementation; as a result of the evolution of the system and its data management; and as a result of developments in processing technology and the availability of related information in the system environment.

However, the broader application and impact of privacy risk assessments may be limited because they currently rely heavily on experience, analogy, and imagination, i.e., risk assessment is more akin to an art than a science. We argue that a more scientific approach to risk assessment can improve the results of privacy impact assessments by making them more consistent and systematic. In addition to measuring and communicating an individual

privacy risk, we see at least five other uses for these privacy risk measurements: quantifying the impact of privacy controls, comparing the impact of different controls, analyzing the trends in privacy risk over time, calculating a system's overall privacy risk from its components, and ranking privacy risks.

To better understand why the risk of a privacy breach is higher when using information technologies for storage, processing, and transmission, one must first understand the basic principles of security in the information world. Information security is the protection of information and its critical characteristics, including all systems used for its transmission, use, and storage. Cybersecurity can be defined by the English word root (cyber), and the meaning is "involving/including computers." In addition, the information security model (CIA triad) assumes that information should be protected in a way that ensures:

- confidentiality – to ensure that only authorized individuals have access to the data;

- integrity – to ensure that the data are not altered and that they arrive from the sender to the recipient in an unaltered form;

- availability – the data must be available at the moment they are needed.

Since the REPRICON project is based on online privacy violation incidents, when explaining the types of attacks, we will specifically describe those that might fall into the category of an online privacy breach.

In human-based attacks, the attacker personally executes the attack by interacting with the target to gather the desired information. In this way, he can influence a limited number of victims.

Software-based attacks are carried out using devices such as computers or cell phones to obtain information from the targets. They can attack many victims in a few seconds. Social

engineering toolkit (SET) is one of the computer-based attacks used for spear phishing e-mails. Social engineering attacks can also be classified into three categories depending on how the attack is carried out: socially, technically, and physically based attacks (Kalniņš, Puriņš, & Alksnis, 2017).

Socially based attacks are carried out through relationships with victims in order to play on their psychology and emotions. These attacks are the most dangerous and successful attacks because they involve human interactions (Gupta, Singhal, & Kapoor, 2016). Examples of these attacks include baiting and spear phishing. Technically based attacks are carried out on the Internet through social networks and online service websites, and they collect desired information, such as passwords, credit card details, and security questions (Kalniņš et al., 2017).

Physically based attacks refer to physical actions performed by the attacker to collect information about the target. An example of such attacks is searching dumpsters for valuable documents.

Social engineering attacks can be divided into several categories depending on their perspective. They can be divided into two categories depending on which entity is involved: human or software. They can also be divided into three categories depending on how the attack is carried out: social, technical, and physically based attacks. By analyzing the various existing classifications of social engineering attacks, researchers can also divide these attacks into two main categories: direct and indirect. Attacks in the first category use direct contact between the attacker and the victim to carry out the attack. They refer to attacks carried out through physical contact, eye contact, or voice interactions. They may also require the attacker's presence in the victim's workspace to execute the attack. Examples of these attacks include physical access, shoulder surfing, dumpster diving, social engineering over the phone, pretexting, asking for somebody by name to come to the help desk, and theft of important documents. Attacks that fall into the indirect category do not require the attacker to be present. The attack can be done remotely via malware software included in

e-mail attachments or SMS messages. The examples of these attacks include phishing, fake software, pop-up windows, ransomware, SMS fishing, online social engineering and reverse social engineering, etc.

Below are some examples of attacks that are of particular interest because they represent a significant invasion of privacy.

Phishing attacks are the most common attacks conducted by social engineers (Gupta et al., 2016). They aim to obtain private and confidential information about targeted individuals through phone calls or e-mails. The attackers mislead the victims to obtain sensitive and confidential information. Fake websites, e-mails, ads, antivirus programs, scareware, PayPal websites, prizes, and free offers are used. For example, the attack can be a phone call or an e-mail from a fake lottery department about winning a sum of money and asking for private data or to click on a link in the e-mail. These data may be credit card information, insurance information, full name, address, first or dream job, mother's name, birthplace, places visited, or other information that could be used to log into sensitive accounts, such as online banking or services (Peotta, Holtz, David, Deus, & de Sousa, 2011).

Pretexting attacks consist of inventing false and convincing scenarios to steal a victim's personal information. They rely on pretexts to make the victim believe and trust the attacker (Ghafir, Prenosil, Alhejailan, & Hammoudeh, 2016). The attack is carried out through phone calls, e-mails, or physical media. The attackers use the publication of information in telephone directories, on public websites, or at conferences where employees from the same field gather to carry out their attack. The pretext may be an offer to provide a service or get a job, ask for personal information, help a friend get access to something, or win a lottery.

Bait attacks are phishing attacks that ask users to click on a link to get free information. They work like Trojan horses, where the attack is carried out via unsecured computer materials, such as storage devices or USB drives with malware that victims find in a coffee shop. When victims insert the USB drive into their computer, the drive behaves like a real Trojan horse

and attacks the computer. This attack performs malicious actions in the background without the victims noticing.

Ransomware attacks are another threat that targets individuals and businesses. Damage amounted to $20 billion in 2021 – 57 times more than in 2015, illustrating the immense financial damage ransomware can cause to businesses. The consequences of a ransomware attack can be more expensive than the ransom itself. Affected companies can suffer the consequences of a ransomware attack for years because they lose their business, customers, data, and productivity. Ransomware attacks restrict and block access to the victim's data and files by encrypting them (Kim, Yoo, Kang, & Yeom, 2017). To recover these files, the victim is threatened by being told that they will be made public unless they pay a ransom (Gallegos-Segovia, Bravo-Torres, Larios-Rosillo, Vintimilla-Tapia, Yuquilima-Albarado, & Jara-Saltos, 2017). This payment must be made with bitcoins, an unregulated digital currency that is difficult to track. There are two ways to analyze a ransomware attack: static and dynamic. Static analysis is performed by highly skilled engineers and programming language specialists who develop programs to analyze and understand the attack so that it can be stopped, or the encrypted files recovered. Dynamic analysis involves remotely observing the malware's functions. It requires that trusted systems can run untrusted programs without damaging the systems. A ransomware attack includes six phases: (1) malware creation, (2) deployment, (3) installation, (4) command and control, (5) destruction, and (6) extortion (Gallegos-Segovia et al., 2017). Malware creation consists of developing ransomware or using existing ransomware to discover a vulnerability in the victim's system and create a backdoor. Deployment consists of spreading the ransomware through the created backdoor bypassing security controls. Installation consists of executing the ransomware and infecting the system. In the command-and-control phase, the ransomware is active if the victim has an Internet connection to communicate with the command center, or passive if it is offline. In the destruction phase, the ransomware starts blocking or encrypting data and freezing screens. The extortion consists of contacting the victim and demanding ransom for the release of the blocked files, setting a deadline. The return of the files after the victim pays is not guaranteed (Everett, 2016). Once a ransomware attack is launched on a computer, the victims have only

three options: (1) pay the ransom to get the encrypted files back; (2) try to restore the files from any backup copies; or (3) lose the data after refusing to pay the ransom (Sittig, & Singh, 2016). All of these are situations have a strong impact on the individual and pose a significant stress event and threat to the individual's mental health and, of course, cause unavoidable material damage.

Attacks with counterfeit software are based on fake websites that trick the victim into thinking that they are well-known and trusted software or websites. The victim enters real credentials on the fake website, which allows the attacker to use the victim's credentials on a legitimate website, for example, to access online bank accounts. An example of these threats is the tabnabbing attack, which consists of a fake web page that looks like the login page of a popular website that the victim usually visits, such as online banking, Facebook, or a company's website (De Ryck, Nikiforakis, Desmet, & Joosen, 2013). Victims enter the credentials while focusing on something else. The malicious user exploits the victim's trust in these websites and gains access to the credentials (Sarika & Paul, 2015).

Reverse social engineering attackers claim to solve a network's problem. This involves three main steps: causing a problem, such as crashing the network; advertising that the attacker is the only person who can solve the problem; solving the problem while obtaining the desired information and disappearing undetected (Beckers & Pape, 2016).

Pop-up window attacks refer to windows that appear on the victim's screen informing that the connection is broken. The user responds by re-entering the credentials, which executes a malicious program that was already installed when the window appeared. This program remotely redirects the credentials back to the attacker. Pop-ups can be, for example, warning messages that are randomly displayed with online advertisements in order to trick the victim into clicking on the window. Pop-ups can also be fake messages informing about a virus detection on the victim's computer. The pop-up asks the victim to download and install the suggested antivirus software to protect the computer. It may also come in the form of fake warnings stating that the computer's memory is full and needs to be scanned and cleaned to

make more space. The victim panics and reacts quickly to fix the problem, which activates the malware software contained in the pop-up window.

In phone/e-mail scam attacks, the attacker contacts the victim via phone or e-mail and asks them for certain information or promises them a prize or free goods. The goal is to get the victim to break security rules or reveal personal information. In addition, cell phone-based attacks can be carried out via phone calls and through short messaging services (SMS) or text messages, known as SMSishing attacks (Ivaturi & Janczewski, 2011). SMSishing attacks use cell phones to send fraudulent messages and texts to victims in order to influence them. They are similar to phishing attacks but are carried out in a different way. The efficiency of SMSishing attacks relies on the fact that the victims can take their cell phones with them wherever they go. A received text message may contain malware even if it was sent by a trusted and known sender. The malware works in the background and installs backdoors through which the attackers gain access to information, such as contact lists, messages, personal e-mails, photos, notes, applications, and calendars. The fraudster can install a root kit to completely control the cell phone (Amro, 2018).

Recently, robocall attacks have emerged, and they are defined as mass-scale calls from computers to targeted individuals with known phone numbers. They target cell phones, home phones, and work phones. A robocall is a device or computer program that automatically calls a list of phone numbers to deliver recorded messages. It is mainly based on Voice-over-the-Internet Protocol (VoIP) to provide various VoIP features, such as interactive voice response and text-to-speech (Tu, Doupe, Zhao, & Ahn, 2016). These calls may be about offering or selling services or solving problems. Help with solving tax problems is a very well-known example of an attack that has increased in intensity in recent years. When a victim answers the call, the phone number is usually stored in the attacker's database. Even after these calls are blocked, the attacker's systems call from other numbers. Robocall attacks have become a serious problem in the U.S. and other countries. The only way to prevent these calls is to not answer unknown phone numbers. There are many other types of attacks, which can be summarized as follows:

Helpdesk attacks: The attacker poses as an authority figure or company employee and calls the help desk to request information or services.

Quid Pro Quo attacks: They are bait attacks in which free services are offered to lure the victim. They demand the exchange of information in exchange for a service or services.

Shoulder-surfing attacks: In these, the victim is observed when entering passwords or sensitive information.

Important document theft attacks: The attacker steals the files from the victim's desk in order to use them for personal purposes.

Social engineering attacks over the Internet: The attacker impersonates a company's network administrator and asks for usernames and passwords.

Risk is usually calculated as a function of probability and impact. There are several proposals for determining the risk of security threats, for example, the guidelines of NIST (2012) or the OWASP Risk Rating Methodology (OWASP, 2022). These are often cited in privacy literature, as security risks can be quite like privacy risks. However, an important difference between security and privacy risks is that privacy risks focus on the harm to individuals (although organizations can turn this into reputational and regulatory risks), whereas harm is of secondary importance when it comes to security risks.

All attackers (threats) seek to exploit system vulnerabilities (digital or analog) to compromise one element (or a combination thereof) within the CIA triad. The extent to which information and the systems used to transmit, process, and store it are compromised can be determined by analyzing the attack surface and the scope and criticality of the resulting vulnerabilities. An attack surface can be defined as the number of directions in which the attackers can penetrate a system and potentially cause damage. For example, in the analog world, it is necessary to lock important data in a safe. A safe may have vulnerabilities of varying

criticality (wall thickness, quality of the locking mechanism, etc.), and the attackers must reach the location in order to steal/exploit it or steal the code. In the digital world, attacks are complex and often very sophisticated (when compared to the data theft in the analog world). The sophistication of the attacks stems from the complexity of information systems in the digital world, which are multi-layered and often heterogeneous (the manufacturers of the components used in the system are different), so successful attacks require thorough preparation by the attacker and a high level of technological knowledge for the attack to be successful.

Storage, processing, and transmission of information with the aid of information and communication technologies (ICT) opens a further direction of attack (via the Internet) that would not exist if the data were stored, used, and transmitted without the use of ICT.

While we have discussed the basic principles of information system security, personal data are the subject of all the activities that lead both to their security and, unfortunately, to attacks. In the digital world, personal data are "disconnected" from the person they identify and are stored, transmitted, and processed in locations not under the direct/permanent control of the individuals to whom they belong. Unfortunately, in most cases, people are not even aware of how their data are managed in the digital world, a concept that some authors also refer to as "information asymmetry." In addition to the personal information that users consciously disclose in the digital world, there are other categories that users mostly share unconsciously: data that the systems "extract" from the users, data that the systems process for the users. The difference between the various types of attacks, when they target a person rather than a system, stems from the medium (with or without ICT) through which the attackers carry out the attacks. If an attacker wants to gather information about a victim whose vulnerability is the attacker himself, they will use various social engineering techniques to obtain the information. In this case, the attackers can use ICT to carry out the attack, but they do not have to.

Once people have been victims of online data theft, it is assumed that their behavior will

change drastically, i.e., their online risk perception will increase. Research has shown that this assumption depends on many factors and that people's responses to risk perception also depend on their financial situation. In addition to the personal variables that affect risk perception, the type of attack a person has been victimized by also affects their risk perception. For example, attacks whose consequences are immediately visible have a greater impact on risk perception than those whose consequences are not immediately visible but only become apparent after a certain time.

4.5. Consumer resilience to online privacy violation: Conceptual model[9]

A consumer's online activity in various dimensions is supposedly affected by the online privacy violation event. The research question is the following: How does a consumer's online activity change after an online privacy breach (stressor), and what are the subsequent outcomes of online consumer activity in the particular dimensions (such as time spent on the Internet, types of transactions performed online, purpose of using the Internet, etc.)? Note that the stressful event of a privacy breach affects individual consumers directly, and the consumers' subjective perceptions of an online privacy breach would be sufficient to determine that a privacy violation occurred.

Privacy violation events could be sorted a posteriori into groups of less and more severe breaches, independent of the subjective classification that may be made by the victim. This could mitigate the risk of wrongly estimated concerns and perceptions. However, it is the estimated concern and perception that results in real behavioral outcomes. Namely, one type of privacy violation that is not perceived as a negative event by individual A might, on the other hand, be perceived as a serious attack on online privacy by individual B. Therefore, the model's exposure to a privacy violation should be a self-assessed, subjective measure.

9 This chapter is a part of the paper Budak et al. (2021).

When affected by the stressor, the individual consumer is, at the same time, resilient to a certain extent (hypothetically, from zero resilience to full resilience). An individual's resilience is formed under the influence of various antecedents. Therefore, the proposed model should include antecedents of online consumer resilience, identify stressful events experienced as a privacy violation, and measure resilience according to adaptation responses in terms of concrete online actions undertaken by a consumer.

Previous studies on individual resilience pointed to several contributing factors, or antecedents, which enhance resilience (Joseph & Linley, 2006; Herrman et al., 2011). Among the variables that have been recognized as important for resilience in different contexts, personality variables are one of the most important. Among the most important antecedents to personal resilience are different psychological factors (e.g., self-esteem, personality traits, locus of control, optimism, self-efficacy) (e.g., Joseph & Linley, 2006; Nakaya et al., 2006), while other factors are of a socio-demographic type, and typically include income, education, age, occupation, and age (e.g., Campbell-Sills, Forde, & Stein, 2009; Carver et al., 2010). In addition, various resilience aspects should also be connected to different psychological well-being factors, as individuals with higher levels of resilience are, in turn, more successful at improving their psychological well-being (Fredrickson, 2001). Finally, recent evidence shows that various personality traits have a sizeable impact on resilience. For example, evidence shows that honesty, emotionality, humility, and openness to experiences influence other personality factors, which then influence resilience development, while extraversion, conscientiousness, and agreeableness have been shown to affect innate and acquired resilience. However, individual resilience is seldom affected only by personality traits (which are, by nature, quite rigid); it is under the influence of wider micro- and macro-environmental factors as well. The examples of micro-environmental factors include social support, family relationships, peers, and stability; while macro-environmental factors generally include community, institutions, and cultural factors (e.g., Luthar & Cicchetti, 2000).

Translated into the model of researching the connection between consumer resilience and privacy violation online, these antecedents are systemized into five groups of variables: psychological

factors, individual attitudes toward Internet usage, individual socio-demographic characteristics and digital literacy, micro-environmental factors, and macro-environmental factors.

4.5.1. Individual psychological factors

Individual values shape the behavior and ideas representing personal life-guiding principles, which are worth considering as antecedents of consumer resilience. In the resilience research literature, numerous protective factors have been identified, including hardiness (Bonanno, 2004), positive emotions (Tugade & Fredrickson, 2004), extraversion (Campbell-Sills et al., 2006), spirituality (Bogar & Hulse-Killacky, 2006), self-esteem (Kidd & Shahar, 2008), and positive affect (Zautra et al., 2005). In investigating the psychological factors as antecedents in our model of consumer resilience to privacy violation in an online environment, self-efficacy emerges as a potentially significant variable (Gu & Day, 2007) for assessing optimistic self-beliefs that help in coping with a variety of stressors in life. Schwarzer & Jerusalem (1995) determined that, if a person is efficiently dealing with unexpected events and solving problems, these abilities might be crucial to confronting a privacy violation event. Additionally, the individuals' locus of control represents the degree to which they believe they have control over event outcomes in their lives (Rotter, 1966). External control orientation refers to the belief that the event outcomes of personal actions stem from external circumstances—faith or luck—while internal control orientation refers to the belief that the outcomes of an individual's actions are driven by personal efforts and decisions. Self-esteem is also included in the model because people with higher self-esteem would not blame themselves for being a victim of an online privacy violation and would feel more capable of dealing with adversity. Some studies claim that individual resilience is rarely attributable to personality traits, yet these factors are widely used in resilience research. Personality traits are psychological factors describing an individual's characteristics that can influence psychological resilience (Nakaya et al., 2006; Campbell-Sills et al., 2006). The "Big Five" concept (e.g., Goldberg, 1993) separates the individuals' personality into five traits: extraversion (social adaptability), openness (to experiences), agreeableness, conscientiousness, and neuroticism (emotional

instability). Certain combinations of these traits can boost the individual's resilience before they even come across a stressful event. Past findings reported that (psychological) resilience was negatively associated with neuroticism, and positively related to extraversion and conscientiousness (Campbell-Sills et al., 2006). Another personality trait is optimism, i.e., maintaining positive expectations for future events or outcomes (Carver et al., 2010). When encountering adversity, maintaining optimism for the future and hope (Snyder, 2000) can provide the stamina to endure and to accept difficulties. Acknowledging the need to adjust is attributed to individual cognitive flexibility. Due to this characteristic, a person sees alternatives, exhibits a willingness to adapt to new situations, and maintains self-efficacy in being flexible (Martin & Rubin, 1995). Active coping skills (Bolger, 1990) are often employed by resilient individuals, including: (i) the cognitive component, actively minimizing the appraisal of threats; and (ii) the behavioral component, including positive statements, facing fears instead of avoiding them, and promoting efforts to ask for others' support.

4.5.2. Individual attitudes toward Internet usage

It is important to differentiate individual traits from individual attitudes. There is evidence in literature that attitudes shape behavior (Glasman & Albarracín, 2006), so the attitudes toward usage should be included in the set of antecedents.

Privacy awareness is defined as the individuals' consciousness regarding the importance of online privacy and threats in the digital environment. Privacy awareness in an online environment encompasses the awareness of privacy policy practices in both public and private sectors (Malhotra, Kim, & Agarwal, 2004; Xu, Dinev, Smith, & Hart, 2008). This relates to the individuals' desire for (sensitive) information control and being familiar with online privacy issues, given that everything posted online stays there forever and can potentially be (mis)used by a third party. The relationship between online privacy awareness and resilience to online privacy violation is speculated to work in the same manner. A higher awareness of online privacy policies and protocols might make Internet users more resilient.

Another factor important to consumer behavior online is the perceived benefits of Internet usage. This is a measure that assesses how beneficial it is for someone to use the Internet, i.e., to be a part of an online community (Malhotra et al., 2004; Dinev & Hart, 2004). Someone with a high personal interest in accessing online information or services might be willing to trade off, i.e., to tolerate potential online privacy violations, thus making the individual more resilient to any online privacy breaches in this sense. These individuals are constantly evaluating the risks and costs of providing their user data online against the benefits of participating in online interactions (Teubner & Flath, 2019).

Resilience to online privacy breeches also relates to the degree of online privacy someone expects or demands. Previous studies have shown a direct correlation between this need and concerns about online privacy levels (Xu et al., 2008; Yao, Rice, & Wallis, 2007), which leads us to speculate that someone with a higher need for privacy in an online environment might be less resilient to any privacy breaches.

Computer anxiety is defined as a general fear of technology and an aversion toward computerization, as well as concern and frustration about the perverse aspects of digitization (Parasuraman and Igbaria, 1990), and it has been shown to negatively affect the users' performance (Thomas, 1994). We speculate that an individual who is already very anxious and frustrated about an increased rate of digitalization would have a relatively low resilience toward online privacy breaches.

Privacy concern in an online environment represents the apprehension and uneasiness of an individual regarding the (mis)use of their sensitive personal data (Lwin, Wirtz, & Williams, 2007), reflecting the degree of the individuals' discomfort when online. We speculate that the individuals with higher levels of concern regarding their privacy online might show lower resilience to privacy breaches online.

The control over personal information in an online environment and unauthorized secondary use of information reflects the individuals' opinions on how their sensitive information should

be managed online. It takes into consideration the individual's attitudes regarding various degrees of control over the collection, sharing, and (mis)use of their private information. Thus, it is regarded as an antecedent to individual resilience to privacy violation. Previous studies investigated the impact of perceived control of an individual (Milne & Boza, 1999) and their perceived ability to manage information (Dinev & Hart, 2004). Thus, we hypothesize that individuals who desire more control over their online information feel more "violated" in case of an online privacy breach, making this individual less resilient.

Online sharing of private information represents an individual's preferences about sharing their private sensitive information online. Past research indicated an indirect association between willingness to provide private information online and privacy concerns (Bandyopadhyay, 2011). Therefore, we theorized that the individuals who are more willing to publicly share their information online would be more resilient to online privacy breaches.

Protective behavior refers to individual actions taken while in an online environment with the goal of protecting one's identity and sensitive information, especially if a person perceives potential threats associated with online activity. According to Lwin et al. (2007), these protective behavior measures might include the fabrication of personal online information (e.g., disguising one's individual identity by deliberately providing inaccurate or incomplete information); adopting various methods to safeguard online personal information (e.g., using various encryption algorithms and anti-tracking software); and purposefully withholding interaction with online content forms (e.g., refusing to fill in forms on particular websites). Milne, Rohm and Bahl (2004) give a few examples of actions individuals might take to protect themselves against online identity theft: filling out forms using isolated accounts, the rejection of website cookies, carefully reading through websites' privacy policies, and adding extra encryption to their e-mails. Hence, behavioral intention factors regarding data fabrication, protection, and withholding should be added to the proposed model. We speculate that the individual who utilizes more protective behavior techniques is more resilient to online privacy violations. In addition, protective behavior processes and actions are more likely to be implemented by the individuals facing higher-than-average risk levels (Ungar, 2011).

4.5.3. Individual socio-demographic factors and digital literacy

The consumers' demographic characteristics can also explain the levels of resilience to privacy breaches in an online environment. Typically, gender, age, education, settlement type, occupation, and household size are included as explanatory variables in the consumer behavior model (Kaapu & Tiainen, 2009; Akman & Rehan, 2014). As such, OECD (2018) identified what it calls the "digital gender divide." Related research shows men to be more interested in digital technology, to be more digitally literate, more likely to take active control, and more willing to take risks (Fogel & Nehmad, 2009; Zhang, Chen & Lee, 2013). Furthermore, some studies indicated that women have an increased likelihood of being exposed to various forms of abuse in an online environment (Grubbs Hoy & Milne, 2010), even though other studies claim that digital harassment is more common in men than women (Nadim & Fladmoe, 2019). Given this research, we speculated that women are likely less resilient to online privacy breaches. In terms of age, we speculated that older Internet users tend to be less resilient to online privacy breaches than younger ones. These young "digital natives" have brighter outlooks on life in general and, more importantly, are more familiar with different data collection practices and financial benefits of an online marketplace. On the other hand, older Internet users show a greater degree of sensitivity and desire to control every aspect of their online information (Zukowski & Brown, 2007). If we look at income as an antecedent of resilience to online privacy breaches, we speculate that high earners are more resilient compared to those who earn less. Past research demonstrated that, in general, high earners show less concern about their online privacy compared to low earners (Zhang et al., 2013; Zukowski & Brown, 2007). Taking a closer look at the achieved education level, past research found higher levels of online privacy concern in individuals with less education (O'Neil, 2001). Finally, regarding the settlement type, European Commission (2020) data for 2019 indicate that about 48 percent of adults living in rural areas in European countries have basic or above basic digital skills. Moreover, Roberts, Beel, Philip, and Townsend (2017) stressed that rural areas differed significantly when it comes to the delivery and use of digital technologies, which is evident in the accessibility of different technologies, IT infrastructure,

or IT education, which then affects their resilience in the digital world. Thus, we speculate that urban residents might show higher levels of resilience to online privacy breaches.

Moving on to the effects of digital skills (digital literacy) on the resilience to online privacy breaches, Vandoninck, d'Haenens and Roe (2013) investigated the factors that influence online resilience among young people in Europe. Their research showed that increased digital literacy levels correlated with greater resilience levels, including better coping strategies. They also emphasized the importance of the role of teachers and peers in increasing the level of online resilience among a younger population. Using a sample of students, similar results were also obtained by Tran et al. (2020), who proved a positive relationship between digital resilience and digital literacy. Moreover, Škrinjarić (2019) showed that an improvement in digital skills correlated with a decline in online privacy concerns. Taking all this into consideration, we expect digital skills (digital literacy) to be positively associated with individual resilience. Individuals with better developed IT competences generally perform a wider range of online activities and spend more time online but in a more secure manner, which might increase their resilience when dealing with potential online threats.

Like digital skills, a few studies suggested that an increased range of Internet user's activities may be inversely associated with online privacy concerns (e.g., Škrinjarić, 2019). Higher levels of familiarization with various online activities should lead to a reduction in computer anxiety and widen the usage of online services. Higher levels of engagement in a variety of online activities and improvements in digital competences should lead to an increased understanding of both the advantages and potential threats in an online environment (Rice, 2006). However, even though increased diversity of online use and digital fluency is generally associated with a reduction of online privacy threats, it may also increase the individuals' exposure to more hidden threats, and hence, resilience may not increase for experienced users. The impact of the consumers' time spent online is speculated to be positively associated with their resilience to online privacy violations.

4.5.4. Micro-environmental factors

Micro-environmental factors comprise various elements of social support available to individuals and are considered one of the most important antecedents of resilience in different circumstances. In this context, social support is understood as the access to or the availability of the assistance of others in times of adversity (Scoloveno, 2016). These factors include family, friends, peers, various organizations, etc. The key aspect of micro-environmental factors, and the main mechanism by way of which they affect the resilience of an individual, is the individuals' ability of interaction using their social support network in times of adversity (Ungar, 2011). In the specific context of resilience to online privacy breaches, these generalized concepts could be contextualized as access to a family member, friend, or peer with high computer literacy, and/or membership in an organization where some members exhibit high computer literacy.

4.5.5. Macro-environmental factors

In general, macro-environmental factors refer to the various laws, customs, and cultural practices that affect the individuals' overall capacity to positively resolve real or perceived issues in times of adversity (Ungar, 2011). This group of factors exists at the community or society level, and is generated by social, political, institutional, and economic forces (Windle, 2011). We posit that social trust, both in institutions and in other people, affects individual behavior (Naef & Schupp, 2009). Further, the consumers exhibiting fewer online privacy concerns believe that the companies selling their products and services online are doing so in a responsible manner, and that the legal regulations of a sufficient enough level to ensure their privacy (Wirtz et al., 2007). The perception of the effectiveness of government regulation of online activities and the opinion that government regulations should be put in place to ensure and promote consumer online privacy (Lwin et al., 2007) could affect consumer resilience to privacy breaches. In exploring consumer behavior online, the level of Internet usage and digitalization present in the living and working environment of an individual

is assumed to affect their resilience to privacy violation online as well. It is reasonable to suppose that the fact that the person is living in a community with well-developed IT infrastructure, surrounded by other Internet users, might nurture an individual's resilience to privacy violation online. To conclude, consumer behavior is governed by several groups of factors, including psychological factors, socio-demographic characteristics, and external factors, stemming from a consumer's micro- and macro-environment.

4.5.6. The outcomes of consumer resilience to online privacy violation

Several outcomes are envisaged depending on an individual consumer's resilience, whereas the consumer's resilience is supposedly formed by antecedents and other determinants. Based on the conceptual model developed by Raab et al. (2015), and the resilience framework of Combaz (2014), five types of reactions to privacy violations will be investigated in the model (Figure 4.3):

- no change in behavior, indicating full resilience to privacy breaches

- full recovery, meaning that an individual bounces back to their normal activity as it was before the stressful event happened

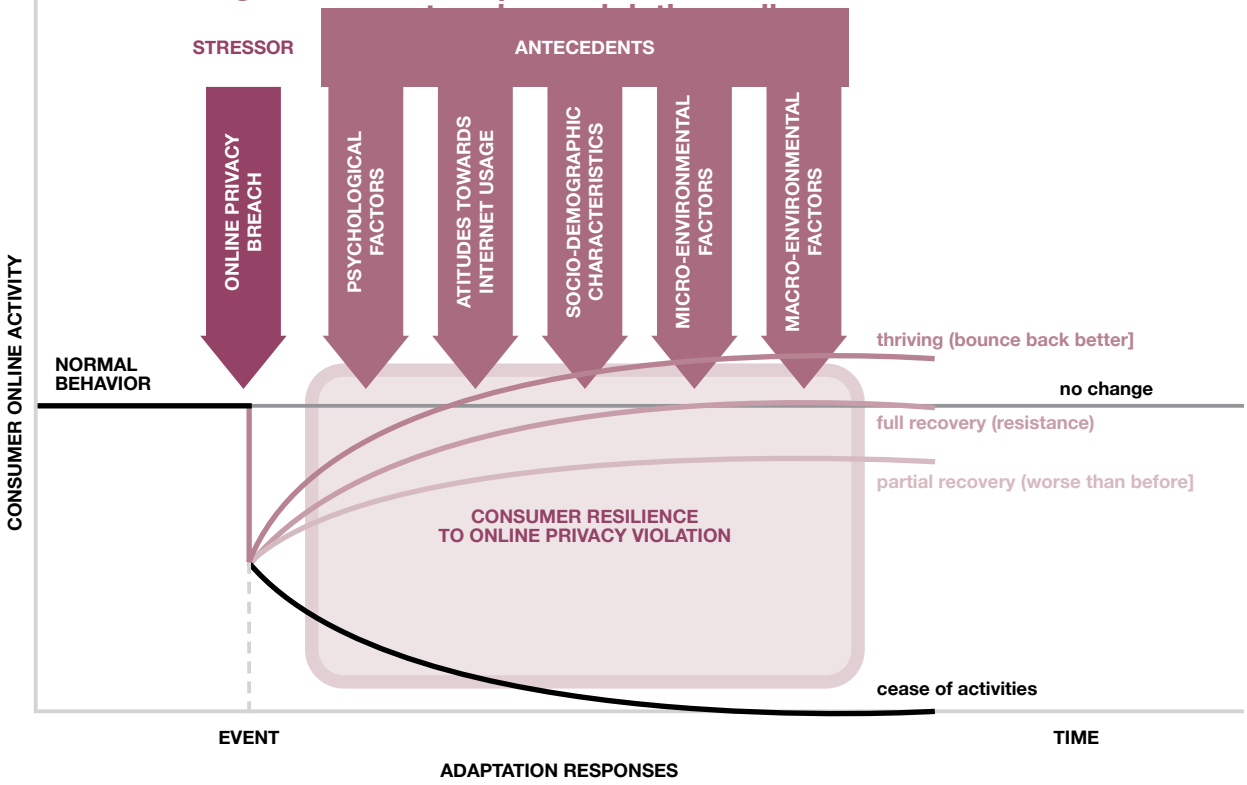
- partial recovery to the worse-than-before level

- recovery to the bounce-back-better level (a hypothetical case in which, after a negative event has passed without severe consequences, the consumer stops worrying about privacy violation and intensifies online activities)

- a complete cessation of previous activities online related to the privacy violation event; with this last reaction being the worst-case scenario of an adaptation response to a

privacy breach, denoting no resilience at all.

Figure 4.3. A conceptual model of consumer resilience



Source: Authors.

The variations in resilience will be measured by observing how consumer behavior recovers after undertaking adaptation actions during a reasonable amount of time. When considering behavioral outcomes, it is imperative to consider the possible inconsistencies between the behavior and the attitudes. Although behavior might recover after a privacy breach incident, attitudes might remain unrecovered and an inconsistency between behavior and attitudes might be observed. This phenomenon is known in literature as the inconsistency between attitude components (Maio, Esses & Bell, 2000; Rosenberg, 1960). Therefore, it might be useful to measure not only the behavior but the attitudes as well, as one of the possible elements of an outcome.

In psychology and social systems, resilience is regarded as the capacity to adjust and flourish and is frequently conceived as a competence that a group or an individual demonstrate when facing a disturbance (stressor), which allows reaching a functionality level designated to be classified as “good” (Longstaff et al., 2013). Hence, this argument corresponds to the “full recovery” outcome in our model. Antecedents are assumed to directly affect resilience; and resilience is a latent variable measured using different scales, which then affects outcomes. However, some antecedents can directly affect outcomes, regardless of resilience (e.g., if one must use the Internet very frequently at work, a change in behavior is unlikely to be observed, though a change in attitudes may be).

5. Survey development

Upon building a model, a customized survey questionnaire was designed and measurement instruments for variables were tested. This stage of survey preparation is of utmost importance because the core of the REPRICON empirical research is the survey. The main purpose of the survey is the assessment of the experiences of 1,000 Internet users in Croatia regarding online privacy breaches; specifically, behavioral outcomes in terms of resilience and consumer adaptation responses. Since the instrument for this phase of research is a structured questionnaire, an initial pool of items should be partly based on the existing measurement scales from the literature and partly on the exploratory phase of research: semi-structured interviews and focus group.

5.1. In-depth semi-structured interviews

Before conducting a survey, theoretical model was tested during the preliminary research based on in-depth semi-structured interviews. The aim of the interviews was to investigate, in more detail, how individuals recover after experiencing some form of privacy violation online, whether they undertook certain actions in respect to privacy violation online and similar issues.

The in-depth semi-structured interview guide was prepared by project team member Edo Rajh (ER), while the in-depth interviews were conducted by the following project members: Jelena Budak (JB), Zvjezdan Penezić (ZP), Edo Rajh (ER), Sunčana Slijepčević (SS), and Bruno Škrinjarić (BŠ). The selection of candidates for the interview was guided by the key precondition that the respondent had experienced some form of privacy violation online. A member of the project team tried to ensure that the total sample of interviews conducted included different age groups of respondents, occupations, and levels of education. in the in-depth semi-structured interviews were conducted during November 2020.

During the interview, questions were directed toward the exploration of topics related to the attitudes about Internet, opinion about privacy violation online which happened to the person who was interviewed and their ability to recover from a negative event. Each interview was performed by one interviewer who asked questions and took notes. All interviews were conducted in Croatian language. In total, 10 interviews were conducted. Basic details about each respondent are shown in the following Table 5.1.

Table 5.1. Basic respondents' data in interviews

No	Interviewer	Date	Duration (mins)	Gender	Age	Education	Occupation	Residence
1	BŠ1	Nov. 18, 2020	30	F	33	Tertiary	Construction architect	Velika Gorica
2	ER1	Nov. 12, 2020	30	M	52	Secondary	Dental technician	Osijek
3	ER2	Nov. 15, 2020	30	F	43	Tertiary	Pharmacist	Zagreb
4	JB1	Nov. 15, 2020	20	F	22	Secondary	Student	Zagreb
5	JB2	Nov. 17, 2020	20	M	55	Tertiary	IT specialist	Zagreb
6	SS1	Nov. 13, 2020	15	F	41	Tertiary	Economist	Zagreb
7	SS2	Nov. 20, 2020	20	M	54	Tertiary	Graphics specialist	Zagreb
8	ZP1	Nov. 17, 2020	10	F	32	Tertiary	Employee in the project office	Zadar
9	ZP2	Nov. 17, 2020	15	M	58	Tertiary	University professor	Zadar
10	ZP3	Nov. 20, 2020	25	M	47	Tertiary	University professor	Zadar

Source: Authors.

On average, the interviews lasted 22 minutes, with the shortest interview lasting 10 minutes and the longest 30 minutes. 50 percent of our interviewees were women, and 50 percent were men. The age of the interviewees ranged between 22 and 55 years, with an average value of 44 years. The average age of interviewed men was higher than that of the interviewed women. The average age of interviewed men was 53 years, as opposed to 34

years for women. 80 percent of the respondents had tertiary education, and 20 percent of the respondents finished secondary school. In-depth interviews included respondents with different occupations (student, pharmacist, economist, graphics specialist, dental technician, construction architect, IT specialist, employee in the project office and two university professors), indicating that the interviews were conducted with people who have different needs when it comes to using the Internet in their professional life, and thus, it is to be assumed that they could also have different levels of computer knowledge and skills and that they use the Internet for different purposes.

Also, in conducting the interviews, the project team took care to conduct them with people from different cities. Thus, the in-depth interview included the respondents from the City of Zagreb (50 percent of the interviews), Zadar (30 percent), Osijek (10 percent), and Velika Gorica (10 percent).

In the next section, the results of this qualitative preliminary research are presented, which served as baseline for the design of the final survey.

We briefly asked the interviewees about their Internet usage and privacy violation online. in the interviews, we specifically focused on investigating how the individuals recover after experiencing some form of privacy violation online and did they experience some change in their behavior due to their previous bad experience.

The results of in-depth semi-structured interviews indicated that respondents use the Internet for various purposes, both of a private and business nature. The respondents generally have positive attitudes about the Internet and can hardly imagine everyday life without using it. Usually, they see the Internet as a means of communication, and a place where much information and data can be found. Interviewees access the Internet through various devices (desktop computers, laptops, mobile phones…) and from different places. Most of the respondents stated that they use the Internet between 4 and 6 hours a day, while only one individual stated that they use the Internet less than 1 hour a day. As could be

expected, those respondents who use the Internet for business purposes use it for a longer time every day.

The respondents faced different forms of privacy violation online related to the use of certain applications (Instagram, Facebook…), the use of e-mail, computer viruses, attempts to charge funds to their credit card and others. Most of the interviewees (40 percent) stated that they were exposed to unauthorized access to the e-mail and/or applications that utilize user accounts at least once during the last three years. Three out of ten interviewees responded that they were exposed to unauthorized supervision of a private data exchange between two subjects (either over phone or via electronic communication) or to close supervision of private data for advertisement purposes. Furthermore, two out of ten interviewees stated that they were exposed to unauthorized use of bank cards/accounts or other online payment methods to acquire a material benefit at the expense of the user, and one interviewee said they were exposed to unauthorized collection and loss of private data due to a computer virus.

Due to the online privacy violation, most of the interviewees stated that they do not longer visit insecure or suspicious Internet sites, or that they do not use those applications related to the privacy violation incident. The respondents said that they are now much more cautious when using the Internet than before they experienced online privacy violation. After the online privacy violation incident, the interviewees dealt with different feelings. Thus, they stated that, following the online privacy violation event, they felt doubts about the safety of using certain programs or applications, surprise, anger, discomfort, and/or concern.

Regarding the activities they undertook because of the online privacy violation they experienced; most respondents stated that they only undertook activities that were closely related to the event. So, they changed the security password, stopped using or reduced their usage of the application or program associated with the event, blocked the card, or stopped shopping online. One person stated that they did not take any action, and that their behavior remained unchanged. However, two out of ten persons stated that this action

did not help them feel better and overcome the online privacy violation incident. Despite this, all interviewees pointed out that their views about the Internet remained the same as before their bad experience. The only change was that some have noticed that their views about the risks and insecurities of using the Internet were now much stronger. Five out of ten interviewees said that the experience of online privacy violation influenced their behavior the most. Three interviewees stated that it affected their feelings the most, and one person explained this as the change in the perception of security and awareness of the possibility that privacy could be violated on the Internet.

When asked about the duration of the change in behavior and how much time they needed to recover after experiencing some form of privacy violation online, five out of ten interviewees stated that the online privacy violation event caused permanent changes in their attitudes and behavior. On the other hand, two persons stated that they changed their behavior only for a very short period, and that they returned to their previous habits of using the Internet. None of the interviewees stated that, after experiencing an online privacy violation, they were in a situation where they had to behave contrary to their views and opinions about the Internet. All ten interviewees stated that their current activities on the Internet were at the same level as before the incident. The only changes relate to the non-use or reduced use of those parts of the system for which they believe are unsafe or related to the online privacy violation event.

5.2. Focus group

The purpose of conducting the focus group was to collect insights about the different aspects of online privacy breaches that might be helpful in the design of the survey instrument. Following the development of the discussion guide, the focus group was organized in December 2020 with eight participants, three men and five women, aged 25 to 50. The participants had from two to 20 years of service and were all employed. The highest completed level of education ranged from a university degree to a Doctor of Science degree. Most of the participants were

from Zadar County, while one participant was from Istria County. All participants were from an urban area. The focus group was held via Zoom platform, in line with the epidemiological conditions that were current at the time, and lasted for two hours. The main results of the focus group are described in detail below.

When it comes to the time that has elapsed since the last potential privacy breach, between one week and six years have passed. Several participants were unable to state the exact time that had elapsed but estimated it to be in the range from six months to one year.

Most participants stated that they use the Internet for communication, both business and private, for searching through databases and/or for finding informative content, online shopping, and, more recently, for organizing business meetings and participating in them. The average daily time spent on the Internet varies from 1.5 hours up to 12 hours a day.

Considering the privacy breach, the participants reported experiencing third-party private data sharing, downloading images from the gallery, and commenting via images, hacking of e-mail accounts, spam, hacking accounts, attempting to access a private e-mail and password changes, logging in to a private mail address. They pointed out that they were most afraid of receiving a large amount of spam e-mails and the hacking of user accounts for various services.

When it comes to the emotions they experience when faced with a particular potential threat, the participants named fear and anxiety as the most common emotions. They experience fear due to the threat that data and documents stored on the Internet could be lost, and that they could be left without financial resources. In addition to fear and anxiety, they experienced anger and helplessness. Also, they felt that the potential violation of privacy was a challenge that they needed to solve.

The violations of privacy affected their online behavior in a variety of ways: the participants have increased caution, they started to handle personal information more carefully, and

have often given up on online shopping or using certain services if they were asked for too much personal information. Furthermore, the participants started to use only verified sites, platforms, or stores, which have already been used by some of their acquaintances and friends or they started to prefer using physical stores. The violations of privacy have led to an imbalance in their rhythm, thoughts, and current activities; they started to feel the lack of privacy and excessive availability of personal data; they started to take care that their actions do not violate their privacy. When warned of a possible problem or threat, they started to feel responsibility toward themselves and their data, and thus, toward others. Here, individuals cited a continuing sense of insecurity.

Despite the feeling of insecurity they experienced, mostly positive emotions have prevailed. When interacting with other colleagues at work, they have experienced everyday satisfaction in working together and helping each other and the responsibility toward the overall collective and business activities.

When thinking about the potential opportunities for privacy breaches in general (thinking about your job, considering the impact of a potential threat on your daily professional and private activities, economic impacts, etc.), most often, the participants cited the experience of fear, discomfort, a certain amount of fear that their online actions could jeopardize the business and private activities that could become public or completely lost.

In terms of behavior, this has had a lasting effect on increasing caution, changing the way one works in an online environment, especially on unknown and unverified sites.

Further concerns were expressed regarding the social networks of younger family members, the protection of digital identity, possible Internet fraud, the growing tendency of society to violate privacy and theft of personal data for profit. Participants believe that, if their value system does not fit into the value system of society, it can contribute to the feeling that someone wants to violate your privacy.

It is interesting to note that GDPR was considered a great help here but that other legislation was not well developed and did not sufficiently protect privacy or personal data. The participants stated that legislation is necessary, but that it was up to us to believe in the efficiency of protection or not. The participants suggested that it may have been necessary to separate physical privacy from digital privacy and to determine the levels of digital privacy (division of digital privacy into the business, personal, community, etc. levels).

Personal factors that mostly contribute to the experience of privacy violations include previous experiences, information, personality traits, education, the level of social network usage and own content published, attitudes, and work experience. As expected, numerous educations warning about the risk of invading privacy increase the subjective notion of online privacy breach.

When it comes to potential privacy threats, individuals would not advise anything but a warning about various privacy breaches. They noticed that the choice of profession is related to many factors, with privacy violation risk being only one of them. Likewise, not all people react equally to privacy breaches. It also depends on how much of their own digital content they have put on the Internet and whether individuals are aware of the possible consequences and speed of content dissemination. Individuals should be more careful and use the Internet responsibly. The advice was to publish as little as possible about their lives online; to understand the digital environment, content sharing and the possibility of different comments from different users; to log out regularly from all social networks and services; to not register for all offered services, and if possible, to hide their identity when online.

Findings about how to deal with stress indicate that a privacy breach should also be reported to the competent authority. Sharing feelings and thoughts with close people and/or professional services is helpful as well because they would advise going to nature and taking a break from technology. If the stress is significant, one should seek professional help.

Finally, one participant commented: “Modern man consciously shares his identity by being

present on the Internet and thus opens up to the possibility of a privacy invasion. This is partly due to his own choices and partly due to the various threats lurking in different software programs, as well as other people using the network. This is similar to life, with the difference being that, instead of the Internet, there are other media, as well as surveillance systems. Here, the question can be raised about the definition of privacy and its boundaries, both personal and public… We can contribute to raising the awareness about possible threats from an early age, as children's online activity is significant. While schools seek consent for an ordinary classroom photography, media, such as press and television, have no problem with posting photos and attachments without consent. It seems like there is an attempt to set boundaries, but no one really knows where to draw a line."

All findings from the focus group, as well as the interviews and literature review were taken into account in the questionnaire design described in the next chapter.

5.3. Questionnaire design

The survey questionnaire was designed by including the items that described all the variables in the REPRICON model. Most of the items were taken from literature by replicating the scales or adapting them in order to better capture the model we aimed to test empirically. For the majority of scales, a five-point Likert scale has been used for capturing the respondents' answers.

The first elimination question (filter, F) was whether a respondent was using the Internet and the second filter question was whether that person had experienced any privacy violation issues on the Internet in the last three years. The interview was stopped if one filter question was answered negatively. By using filter questions, we assured that the survey data were collected from the target population only.

An open-ended question asking the respondents to describe the online privacy violation

incident (OPVI) followed.

In order to determine the appropriate scale to measure resilience (RES), we have consulted the work of Windle, Bennett, and Noyes (2011), who analyzed the total of 19 resilience scales and rated three of them as superior in terms of psychometric characteristics: (1) the Connor-Davidson Resilience Scale (CD-RISC; Connor & Davidson, 2003); (2) the Resilience Scale for Adults (RSA; Friborg, Hjemdal, Rosenvinge, & Martinussen, 2003); (3) the Brief Resilience Scale (BRS; Smith, Dalen, Wiggins, Tooley, Christopher, & Bernard, 2008). The latter one was chosen because of the conceptual clarity and resilience definition used by the authors (Smith et al., 2008). A relatively small number of items, 6 of them, was adequate to be included in the larger questionnaire and for interviewing adult persons. Three statements in the original 6-item scale were reciprocal and therefore, had to be re-coded. We finally adopted the original BRS items to express the recovery after an online privacy violation incident (Vagias, 2006).

The consumers' attitudes (ATT) toward Internet after an online privacy violation incident were measured using four items developed by the authors to measure the change in (i) Internet usage, (ii) the level of cautiousness when online, (iii) the range of online activities and (iv) the general attitude toward the Internet.

The intensity of using the Internet (WEB) was checked using an open question measuring the hours spent on the Internet on a typical day, for both private and work purposes. The diversity of the activities performed online, ranging from the simple to the more sophisticated ones (including social networks, e-banking, e-shopping, e-public services, etc.) is captured by 15 statements examining how often a person performs the 15 proposed types of online activities (from 1 – never to 5 – very often). The separate yes or no question was about online buying habits, asking if the person had ever bought goods or services on the Internet (EBUY).

Individual Internet skills (SKILL) were measured by six items, similar to the scale used by Škrinjarić (2019), representing the gradation from the simplest to the more complex Internet-related tasks the user can perform.

In order to measure the five personality traits (PT), the original OCEAN Big Five personality traits scale was used, as shortened in Rammstedt and Oliver (2007).

In order to measure the optimism (OPT) and pessimism (PES) variables, we have borrowed the original Optimism-Pessimism (O-P) measurement scale developed by Chang (as described in Chang, Maydeu-Olivares, & D'Zurilla, 1997), containing six items to measure optimism and nine items to measure pessimism. The original O-P scale (Chang et al., 1997) has been adapted for this research by reducing the number of items. Three items from the original optimism scale (opt 1–3) and three items from the original pessimism scale were used in the questionnaire.

The social support (SS) variable was measured by adapting the Oslo 3 Social Support Scale that originally consisted of three items (Kocalevent et al., 2018) asking about the accessibility of practical help. The scale was adapted by aggregating the availability of practical help in using the Internet into one question (the answers rating the difficulty of obtaining help scored from 1 – Very difficult to 5 – Very easy).

Self-esteem was measured using a single item scale developed by Robins, Hendin, and Trzesniewski (2001).

The self-efficacy scales used in personality and psychological studies are mostly derived from the General Self-Efficacy Scale developed by Sherer, Maddux, Mercandante, Prentice-Dunn, Jacobs, and Rogers (1982). We adapted the later Generalized Self-Efficacy scale from Schwarzer, Bäßler, Kwiatek, Schröder, and Zhang (1997) to better measure general self-efficacy, and to be able to adequately measure self-efficacy (SEF) in the specific resilience to privacy violation online context.

Online privacy awareness (OAW) was measured using three items taken and adapted from Xu et al. (2008) (oaw1), and Malhotra et al. (2004) (oaw2 and oaw3). It focuses on how well an Internet user is informed about and interested in online privacy protection issues.

The level of social trust (ST) was measured based on four statements that reflect the respondents' level of trust in people, the state, the local public institutions, and their community, in line with Naef and Schupp (2009).

The General Internet attitude scale (GIAS) measures the individuals' general attitude toward the Internet. The General Internet attitude scale used in REPRICON is a single-item variable based on Joyce and Kirakowski (2015), adapted from one item from the theory of planned behavior attitude scale (Ajzen, 1991; Yoon, 2011).

The perceived online benefits (BNF) of online services or information from the Internet compared to the online privacy concern were measured using two statements taken and adopted from Dinev and Hart (2006).

Digitalization anxiety (DA) was measured using two statements derived from the computer anxiety measurement scales based on the work of Parasuraman and Igbaria (1990). The items were adapted to explore the perceptions of the negative effects and threats of digitalization.

The intention to use digital public services (DPS) and the intention to use local digital public services (LDPS) were measured using two items each. Those items were adapted from Venkatesh and Davis (2000) intention to use scale.

The online privacy concern (OPC) variable was initially based on the scale from Smith, Milberg, and Burke (1996). It was one of the first scales dealing with the concern for information privacy, developed to measure the collection, errors, secondary use, and unauthorized access to information as the dimensions of an individual's concern about privacy. Our OPC scales were also adapted from Malhotra et al. (2004) construct of Internet users' information privacy concerns. It reflects the concerns in the online environment better because it comprises the attitudes toward collecting personal information, the control over personal information and the awareness about privacy practices of companies gathering personal information (Anić et al., 2018). We have borrowed three items from the original scale, covering various aspects of

online privacy concerns. The respondents were asked to rate their general concerns about online privacy, concerns about the extensive collection of privacy information online and concerns about privacy violation online.

The perceived degree of regulatory control (REG) and its efficiency was measured using two items taken from Lwin et al. (2007). The items were adapted to reflect the opinion about whether the existing laws and government actions were sufficient to protect against privacy violation online.

The willingness to share private information online (SH) was investigated by asking about the different types of information on different sharing platforms, such as social networks. This variable was adopted from Anić et al. (2018). We asked if people posted private information on the Internet, post the information about their current location or accompanying persons publicly, or provide their credit card number when buying online.

Protective behavior (PB) was assessed using a set of six statements asking how often a respondent behaved in some of the listed ways when on the Internet (Wirtz et al., 2007). The answers were provided on the five-point scale ranging from never to very often. Some of the examples of behavior included giving false responses, using another e-mail address to hide their real identity, using the private browsing option, refusing to provide excessive personal information to untrustworthy websites, etc.

The intent to adopt new technologies (IT) was investigated by asking about the likelihood of being an early user of new online services or technologies as soon as they became available (as used in Wang, Dacko, and Gad, 2008).

Finally, the demographic characteristics of individual respondents (D) were expressed by asking them about their age (in years) and education level (primary school or lesser level, secondary or tertiary education or master/doctoral degree). The interviewer noted the gender of the respondent and asked them about the number of household members. This enabled

us to calculate the average income per capita since, later on, they were asked the question about the total net average monthly income of their household. In order to avoid not being given an answer to this delicate question, the answers that were offered were systemized into ten categories corresponding to the income brackets in Croatia, expressed in the formerly official local currency kuna.

Seeing as online privacy concerns might depend on the job performed and the employment status, we asked the respondents about their occupation, divided into five categories corresponding to the international classification (owner/ sole proprietorship, self-employed, manager/official, professional, and technician/clerk) and whether they were unemployed, a student or retired. Here, we offered them an option of an open question to provide the "Other" answer as well.

Finally, regional distribution was recorded in the questionnaire by the interviewer who knew, in advance, which county telephone number extension they have dialed. The respondent had to name their settlement and provide details on the settlement size in terms of the number of inhabitants (four size brackets were provided).

The codebook for 26 variables is presented in Table 5.2 and the questionnaire with coded items is provided in Appendix 2 and Appendix 3.

Table 5.2. The codebook for variables in the REPRICON model questionnaire

Code	Variable
F	Filter questions
OPVI	Online privacy violation incident description
RES	Resilience to online privacy violation
ATT	Behavior and attitude change after an online privacy breach
T	Time spent online for private and work-related reasons
WEB	Diversity of online activities
SKILL	Internet skills
PT	Personality traits
OPT	Optimism
PES	Pessimism
SS	Social support
SE	Self-esteem
SEF	Self-efficacy
OAW	Online privacy awareness
ST	Social trust
GIAS	General Internet attitude scale
BNF	Perceived online benefits
DA	Digitalization anxiety
DPS	Digital public services
LDPS	Local digital public services
OPC	Online privacy concern
REG	Degree of regulatory control
SH	Sharing private information online
PB	Protective behavior
IT	Intent to adopt new technologies
EBUY	Online purchases
D	Demographics

Source: Authors.

5.4. Questionnaire pre-testing

The main research instrument is a highly structured questionnaire. The questionnaire consists of three parts. The first part of the questionnaire consists of questions about the use of Internet and the experience of online privacy violation incidents. The second part of the questionnaire consists of the questions that measure the variables from the theoretical model tested by this research. In this part of the questionnaire, the already-developed measurement scales from literature were used, but they have been adjusted to the research context. The last, third part of the questionnaire refers to the socio-demographic characteristics of the respondents.

After the questionnaire had been designed, the first pilot test was conducted on the sample of 9 respondents, with the aim of testing the clarity of the questions, identifying possible problems during the survey, and the duration of the survey. Furthermore, the duration of the survey in the CATI environment was examined on a sample of 30 respondents. After the necessary changes to the questionnaire have been made to increase the clarity of the questions and to adjust the duration, another pilot study was conducted on the sample of 10 respondents. The final pilot testing showed that the average duration of the survey was about 21 minutes, and that the clarity of the questions was satisfactory. The original version of the final questionnaire used in the survey in Croatian is enclosed as Appendix 2 and the translated English version as Appendix 3.

5.5. Sampling and field research

The research was conducted on the quota sample of Internet users in Croatia who were older than 18 according to the Eurobarometer study from January 2019.[10] The sample was two-way, stratified by region and settlement size. The appropriate quantity of telephone numbers was selected randomly from the telephone database and uploaded to the system. Each

10 European Commission and European Parliament, Brussels (2019). Eurobarometer 91.1 (2019). GESIS Data Archive, Cologne. ZA7561 Data file Version 1.0.0, https://doi.org/10.4232/1.13317

telephone number was called three times before its final removal from the list.

The fieldwork was contracted with Hendal Agency. Prior to the start of the fieldwork, a briefing for all interviewers and supervisors participating in the project was held. The following topics were included in the briefing:

- procedure of selecting the respondent within the household
- general information on the project and the procedure of introducing the project to the respondent
- questionnaire – going through and explaining each survey question with regard to the following aspects: content, type of question, possible answers, and specific interviewer's instructions, if present.

The fieldwork was conducted using Computer Assisted Telephone Interviewing (CATI). Hendal Agency's CATI system uses Warp-IT software that enables questionnaire programming, database management, and quality control. The questionnaire was programmed and tested before the pilot interviews. The main body of fieldwork was conducted between January 19 and February 24, 2021, with 23 interviewers conducting the interviews. The response rate was 4.6 percent and the final questionnaire length was 23.32 minutes on average. In the total net sample of 1007 Internet users who had experienced online privacy violation, the quota of at least 66 percent of respondents buying online was met.

The quality of the interviewers' work was conducted by four supervisors who listened to the interview during its conduction. 25 percent of each interviewer's work was controlled. In case of any deviation from the standard procedure, the answers were removed from further processing. Additional data consistency checks were made by the project manager during data processing.

Sample characteristics in terms of gender, age, number of people living in the household of the respondent, education and occupation of respondent, household income, region (counties and NUTS2 regions in Croatia), and settlement size of the respondent's place of residence are presented in Table 5.3.

Table 5.3. Sample structure

Variable	Frequencies (N=1,000)	Relative frequencies	St. dev.	Min.	Max.
Gender					
Female	513	51%	0.50	0	1
Male	487	49%	0.50	0	1
Age*		43.31	15.88	18	86
Age categories					
18–29	253	25%	0.43	0	1
30–39	184	18%	0.39	0	1
40–49	186	19%	0.39	0	1
50–59	187	19%	0.39	0	1
60+	190	19%	0.39	0	1
Number of people in household*		3.35	1.42	1	10
Education					
Primary or less	20	2%	0.14	0	1
Secondary	518	52%	0.50	0	1
Tertiary	426	43%	0.49	0	1
PhD or post-graduate	36	4%	0.19	0	1
Occupation of respondent					
Self-employed	50	5%	0.22	0	1
Manager	45	5%	0.21	0	1
Professional	160	16%	0.37	0	1
Technician/clerk	191	19%	0.39	0	1
Worker	191	19%	0.39	0	1
Retired	159	16%	0.37	0	1
Student	111	11%	0.31	0	1
Unemployed	93	9%	0.29	0	1

Variable	Frequencies (N=1,000)	Relative frequencies	St. dev.	Min.	Max.
County of the respondent					
Zagreb	93	9%	0.29	0	1
Krapina-Zagorje	24	2%	0.15	0	1
Sisak-Moslavina	50	5%	0.22	0	1
Karlovac	34	3%	0.18	0	1
Varaždin	43	4%	0.20	0	1
Koprivnica-Križevci	28	3%	0.17	0	1
Bjelovar-Bilogora	26	3%	0.16	0	1
Primorje-Gorski Kotar	89	9%	0.28	0	1
Lika-Senj	8	1%	0.09	0	1
Virovitica-Podravina	9	1%	0.09	0	1
Požega-Slavonia	14	1%	0.12	0	1
Brod-Posavina	19	2%	0.14	0	1
Zadar	44	4%	0.21	0	1
Osijek-Baranja	96	1%	0.29	0	1
Šibenik-Knin	15	2%	0.12	0	1
Vukovar-Srijem	15	2%	0.12	0	1
Split-Dalmatia	124	12%	0.33	0	1
Istria	48	5%	0.21	0	1
Dubrovnik-Neretva	25	3%	0.16	0	1
Međimurje	33	3%	0.18	0	1
City of Zagreb	163	16%	0.37	0	1
Region (NUTS2) of respondent					
Pannonian Croatia	263	26%	0.44	0	1
Adriatic Croatia	353	35%	0.48	0	1
City of Zagreb	163	16%	0.37	0	1
Northern Croatia	221	22%	0.42	0	1
Settlement size					
10,000 or less	309	31%	0.46	0	1
10,001–50,000	296	30%	0.46	0	1
50,001–100,000	79	8%	0.27	0	1
More than 100,000	316	32%	0.47	0	1

Note: * Here we present averages rather than frequencies. As of January 1, 2023, Croatia adopted the euro as its official currency with the official fixed exchange rate 1 EUR = 7.53450 HRK.

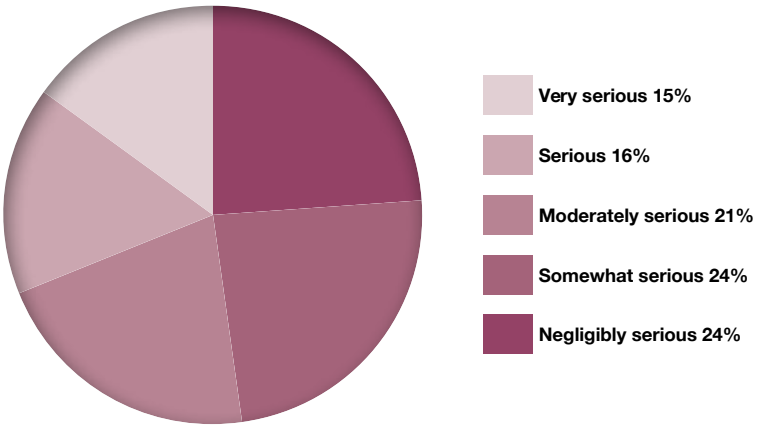
Source: Authors.

6. Descriptive statistics and scale validation

This chapter presents the basic descriptive statistics of the data collected by the survey on a sample of 1,007 respondents who, according to their subjective assessment, experienced an online privacy violation incident. The values of the variables were in most cases measured by the Likert scale of grades from 1 to 5, with 1 representing the weakest and 5 the highest score. The exceptions are (i) the question asking for a description of the last incident of online privacy violation, (ii) the question in which the respondent assesses how much time they actively spend on the Internet, and (iii) the questions that reflect the socio-demographic characteristics of respondents. The descriptive statistics of latent variables (for each item in the questionnaire) is given in Appendix 4.

For the whole sample, 30 percent of the respondents consider that the case of online privacy violation they had was very serious or serious, while 24 percent of them consider the event as only negligibly serious (Figure 6.1).

Figure 6.1. How serious was the online privacy violation incident for you?



Note: In percentage of respondents.

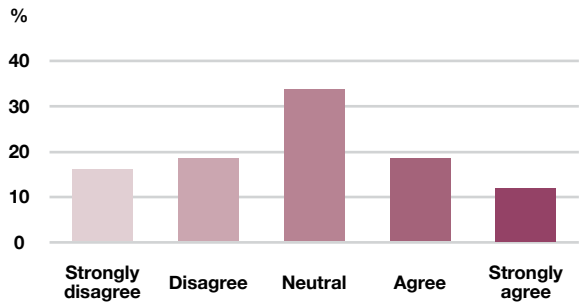
Source: Authors.

The survey measured six dimensions of resilience to online privacy violation (Figures 6.2–6.7). Every third respondent answered that they did not bounce back quickly after the most

recent online privacy violation incident. Almost half of the respondents stated that they had a hard time making it through after the most recent online privacy violation incident, and 21.9 percent of respondents needed a long time to recover from the most recent online privacy violation incident. 17.4 percent of respondents stated that it was hard for them to snap back when the most recent online privacy violation happened. 55 percent of respondents said that they came through the most recent online privacy violation incident with little trouble.

The results indicate that the mean level of resilience to online privacy violation is 3.43.

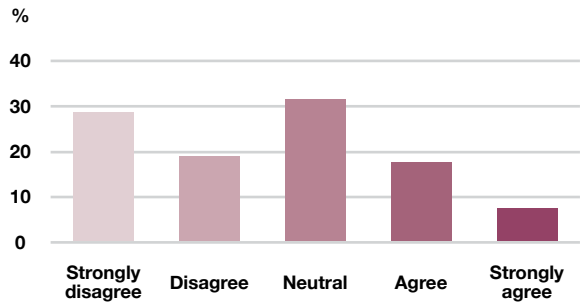
Figure 6.2. I bounced back quickly after the most recent online privacy violation incident.



Note: In percentage of respondents.

Source: Authors.

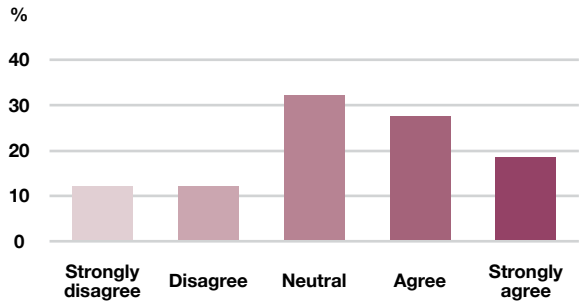
Figure 6.3. I had a hard time making it through after the most recent online privacy violation incident.



Note: In percentage of respondents.

Source: Authors.

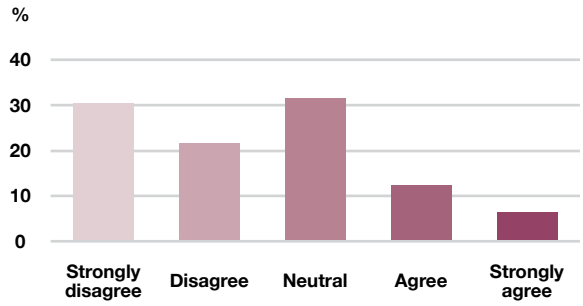
Figure 6.4. It didn't take me long to recover from the most recent online privacy violation incident.



Note: In percentage of respondents.

Source: Authors.

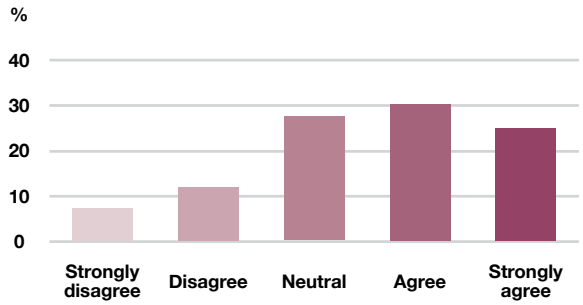
Figure 6.5. It was hard for me to snap back when the most recent online privacy violation happened.



Note: In percentage of respondents.

Source: Authors.

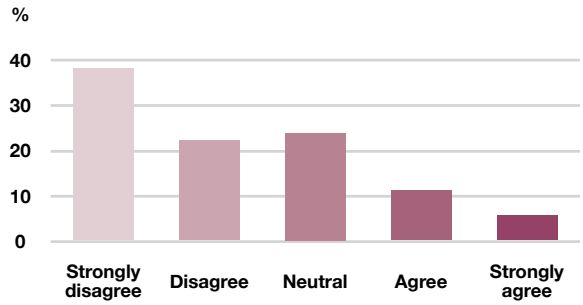
Figure 6.6. I came through the most recent online privacy violation incident with little trouble.



Note: In percentage of respondents.

Source: Authors.

Figure 6.7. It took me a long time to get over the most recent online privacy violation incident.

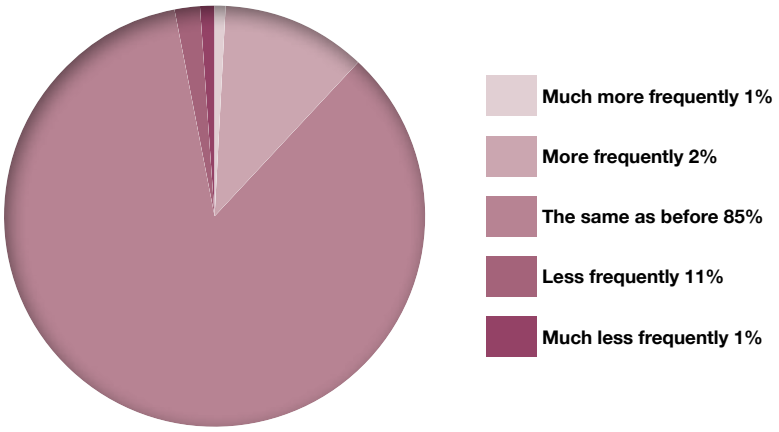


Note: In percentage of respondents.

Source: Authors.

In the survey, we also analyzed the impact of online privacy breach on change in the respondent's behavior and attitudes. The results are shown in Figures 6.8 to 6.11.

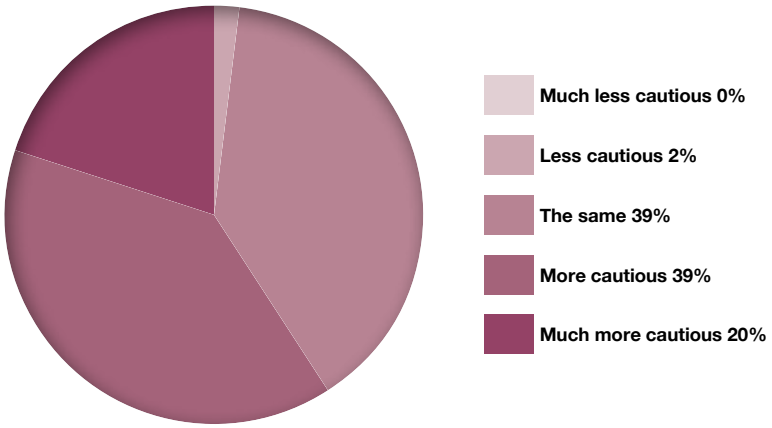
Figure 6.8. After the online privacy violation incident, I use the Internet



Note: In percentage of respondents.

Source: Authors.

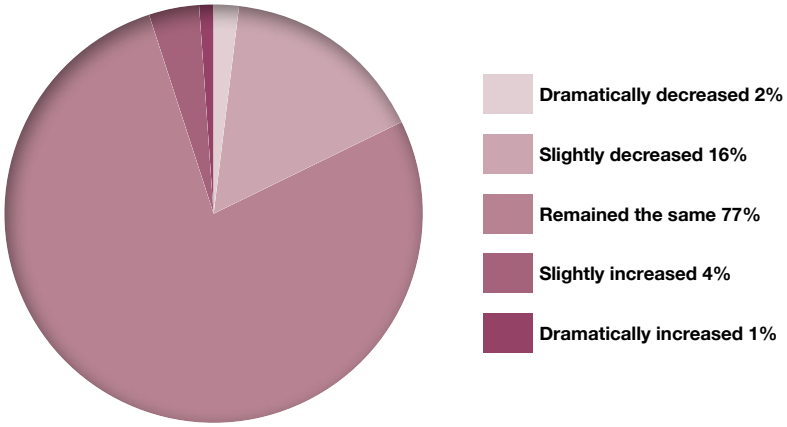
Figure 6.9. After the online privacy violation incident, I am _____ cautious on the Internet



Note: In percentage of respondents.

Source: Authors.

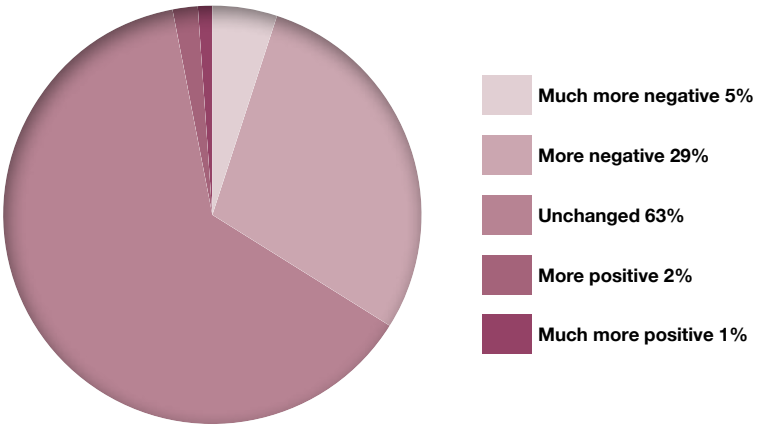
Figure 6.10. After the online privacy violation incident, the range of activities I perform on the Internet has



Note: In percentage of respondents.

Source: Authors.

Figure 6.11. After the online privacy violation incident, my attitude toward the Internet became:



Note: In percentage of respondents.

Source: Authors.

The results indicate that respondents generally continued to use the Internet as before the online privacy violation incident. 11.1 percent of respondents reduced the use of Internet after the incident, and 1.7 percent of them use the Internet much less than before. 84.9 percent of respondents use the Internet as before the online privacy breach. However, the attitudes of respondents have changed. Almost 60 percent of respondents are more cautious on the Internet than before the online privacy violation incident. In 77 percent of respondents, the range of activities they perform on the Internet remained the same as before the incident. However, 18.5 percent of respondents decreased or dramatically decreased the range of activities they perform on the Internet. More than 34 percent of respondents have a more negative attitude toward the Internet after the online privacy violation incident.

Table 6.1. Use of Internet for various activities

Variable	Mean	St. dev.	Min.	Max.
Internet activities				
Internet activities – search engines	4.30	0.84	1	5
Internet activities – chat	4.13	1.05	1	5
Internet activities – e-mails	4.01	1.04	1	5
Internet activities – daily news	3.75	1.05	1	5
Internet activities – social networks	3.65	1.34	1	5
Internet activities – streaming	3.44	1.19	1	5
Internet activities – banking	3.18	1.41	1	5
Internet activities – driving maps	2.87	1.15	1	5
Internet activities – calls	2.86	1.27	1	5
Internet activities – public services	2.76	1.24	1	5
Internet activities – shopping	2.50	1.28	1	5
Internet activities – download	2.45	1.23	1	5
Internet activities – games	2.34	1.34	1	5
Internet activities – courses	2.32	1.41	1	5
Internet activities – online forums	2.00	1.1	1	5

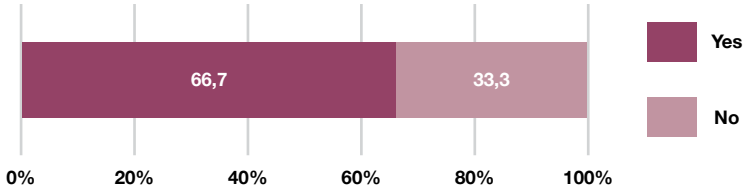
Note: 1 – Never; 5 – Very often.

Source: Authors.

The data in Table 6.1 show for what purposes the respondents use the Internet and to what extent. The results of the survey indicate that respondents mostly use the Internet to search for general information. As many as 87 percent of them use search engines often or very often and only 1.2 percent of the respondents never use search engines to find information online. Also, more than 70 percent of respondents often or very often use the Internet to receive and send e-mails and for chat or instant messaging services.

The Internet is the least used to participate in online forums. Every ninth respondent who has had an online privacy violation incident uses the Internet frequently or very often to participate in online forums and 43 percent of respondents never participate in online forums.

Figure 6.12. Internet shopping



Note: In percentage of respondents.

Source: Authors.

67 percent of respondents use the Internet to buy products or services (Figure 6.12). Every third person who had an online privacy violation incident does not use the Internet for shopping.

The data in Table 6.2 show how respondents rate the level of their Internet skills. Thus, 59.5 percent of respondents think that they can use Internet browsers extremely well, and 55.4 percent of respondents think that they can open a new e-mail or social network address extremely well. 43.3 percent of respondents believe that they can work very well with/edit bookmarks and 39.5 percent of them think that they can save content from websites to their devices very well. The smallest number of respondents have the knowledge needed to administer and create websites. Thus, 28.6 percent of respondents believe that they can use programming languages to create or administer a website well or very well and 19.4 percent of them think that they can create a basic website well or very well.

Table 6.2. Level of Internet skills

Variable	Mean	St. dev.	Min.	Max.
Internet activities				
Internet skills – browser navigation	4.39	0.91	1	5
Internet skills – registering a new account	4.26	1.05	1	5
Internet skills – bookmarks	3.85	1.35	1	5
Internet skills – saving content	3.71	1.39	1	5
Internet skills – website administration	2.54	1.44	1	5
Internet skills – website creation	2.15	1.36	1	5

Note: I can perform Internet-related tasks: 1 – Not at all; 5 – Very well.

Source: Authors.

Within the survey, we also investigated the personality traits of the respondents. Women find themselves to have a higher level of general trust in other people, have more artistic interests, characterize themselves as more social and more conscientious than men. On average, 15.1 percent of respondents consider themselves to be someone who is reserved, 8.9 percent think that they tend to be lazy, and only 5.4 percent see themselves as a person who tends to find fault with others. On the other hand, seven out of ten respondents find themselves to be someone who does a thorough job and who is sociable.

Looking at the average division of personality into five traits (extraversion, agreeableness, conscientiousness, neuroticism, and openness), most of the respondents find themselves to be conscientious (mean value 3.93). On the other hand, neuroticism is scored much lower, with a mean value of 2.57.

Table 6.3. Personal characteristics of respondents

Variable	Mean	St. dev.	Min.	Max.
Personality traits				
Personality traits – extraversion 1	2.57	1.01	1	5
Personality traits – agreeableness 1	3.55	0.83	1	5
Personality traits – conscientiousness 1	2.08	1.04	1	5
Personality traits – neuroticism 1	3.41	0.99	1	5
Personality traits – openness 1	3.36	1.2	1	5
Personality traits – extraversion 2	3.97	0.92	1	5
Personality traits – agreeableness 2	1.91	0.92	1	5
Personality traits – conscientiousness 2	3.95	0.84	1	5
Personality traits – neuroticism 2	2.55	1.07	1	5
Personality traits – openness 2	3.35	1.17	1	5
Extraversion (item mean)	3.70	0.86	1	5
Agreeableness (item mean)	3.82	0.72	1.5	5
Conscientiousness (item mean)	3.93	0.81	1.5	5
Neuroticism (item mean)	2.57	0.91	1	5
Openness (item mean)	2.99	0.69	1	5
Optimism				
Optimism – item 1	3.73	0.84	1	5
Optimism – item 2	3.75	0.87	1	5
Optimism – item 3	3.56	0.8	1	5
Optimism (item mean)	3.68	0.71	1	5
Pessimism				
Pessimism – item 1	2.38	1.05	1	5
Pessimism – item 2	2.48	0.96	1	5
Pessimism – item 3	2.65	1.03	1	5
Pessimism (item mean)	2.50	0.86	1	5
Self-esteem	3.72	0.89	1	5
Self-efficacy				
Self-efficacy – item 1	3.73	0.82	1	5
Self-efficacy – item 2	3.87	0.79	1	5
Self-efficacy – item 3	4.11	0.75	1	5
Self-efficacy – item 4	3.89	0.83	1	5
Self-efficacy (item mean)	3.9	0.63	1.8	5
Social trust				
Social trust – people	3.39	0.93	1	5
Social trust – state public institutions	2.35	1.05	1	5
Social trust – local public institutions	2.5	1.03	1	5
Social trust – local community	3.32	1.03	1	5
Social trust (item mean)	2.89	0.77	1	5
Online privacy awareness				
Online privacy awareness – item 1	2.85	1.05	1	5
Online privacy awareness – item 2	4.12	1.07	1	5
Online privacy awareness – item 3	4.31	0.88	1	5
Online privacy awareness (item mean)	3.76	0.65	1	5
General Internet attitude scale	3.79	0.84	1	5

Note: 1 – Absolutely no; 5 – Absolutely yes.

Source: Authors.

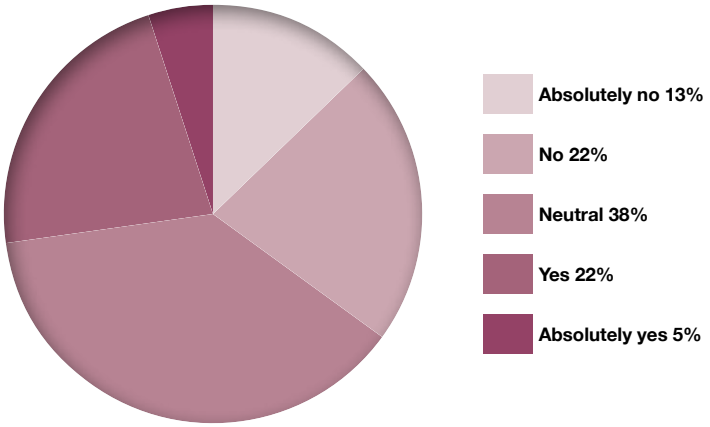
We also investigated the level of optimism and pessimism of respondents. The respondents on average find themselves more optimistic than pessimistic. The mean value of optimism of respondents is 3.7, while the mean value of pessimism is 2.5. Therefore, about half of the respondents who have experienced online privacy violations always look at life from a brighter side, are optimistic about their future, and believe that in general things always turn out well. On the other hand, between 11 and 16 percent of respondents find that things never go the way they want, that it is better to expect failure, and they rarely expect anything good to happen.

The mean value of self-esteem of respondents is 3.7, showing that respondents, on average, have a high level of self-esteem. Only 8.5 percent of respondents find that they do not have a high level of self-confidence.

The level of social trust of respondents includes respondents' subjective assessment of trust in people, in local public institutions, in public institutions at the central government level, and in the local community. The mean value of social trust is 2.9, which is the result of greater trust of respondents in people and the local community, and a lower level of trust in public institutions.

Furthermore, one-third of the respondents stated they were not familiar with privacy issues and the solutions that companies and the government employ to ensure online privacy. In addition, 77.5 percent of respondents believe that websites that request use of personal data and information should disclose the way data are collected, processed, and used, and 84.1 percent of respondents believe that online privacy policies should have clear and conspicuous disclosures (Figures 6.13 to 6.15 and Table 6.3).

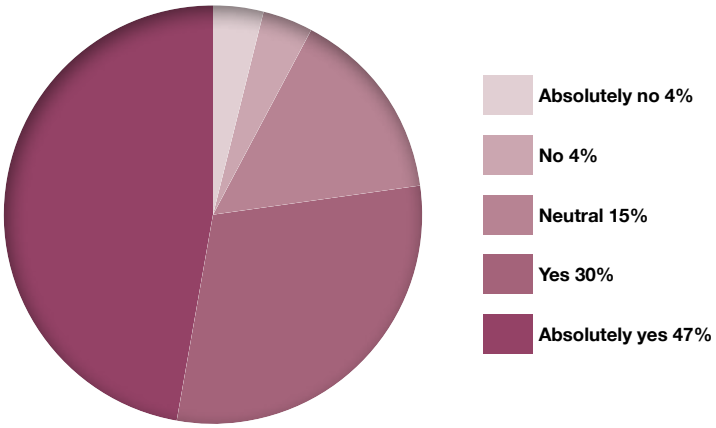
Figure 6.13. I keep myself updated about privacy issues and the solutions that companies and the government employ to ensure our privacy.



Note: In percentage of respondents.

Source: Authors.

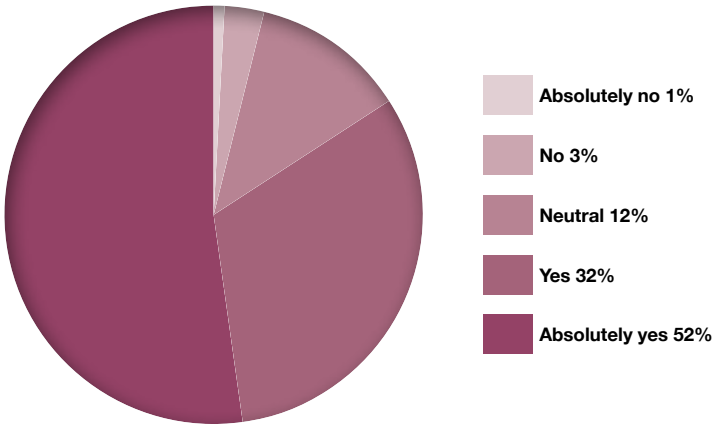
Figure 6.14. Websites seeking information online should disclose the way the data are collected, processed, and used.



Note: In percentage of respondents.

Source: Authors.

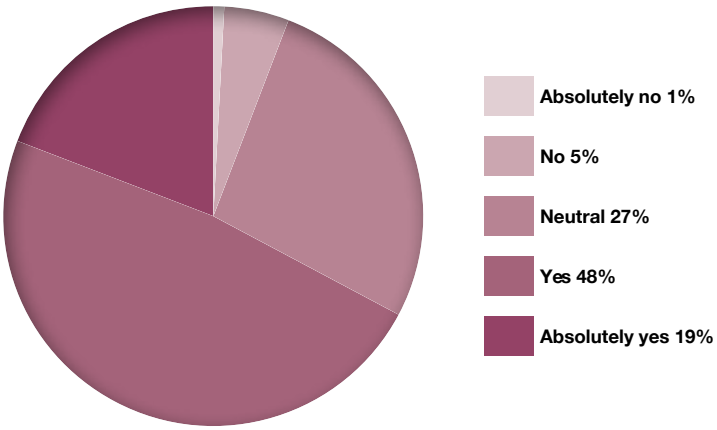
Figure 6.15. A good online privacy policy should have a clear and conspicuous disclosure.



Note: In percentage of respondents.

Source: Authors.

Figure 6.16. I have a positive attitude toward the Internet.



Note: In percentage of respondents.

Source: Authors.

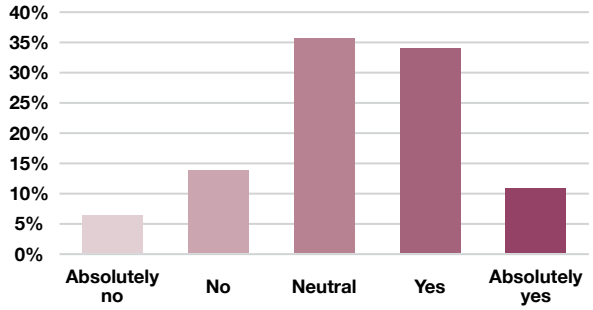
Despite the online privacy violation incident they had, 67 percent of respondents have a positive attitude toward the Internet. Only 6.1 percent of respondents have a negative attitude toward the Internet. The mean value of general Internet attitude is 3.8 with a standard

deviation of 0.8 (Figure 6.16 and Table 6.3). On average, male respondents have a slightly more positive attitude toward the Internet than female respondents who have experienced an online privacy violation incident. The mean value for male respondents is 3.8 and for female respondents 3.7.

Respondents largely stated that their need to obtain certain information or services from the Internet outweighs their concerns about online privacy. 46.7 percent of respondents have such an attitude, while as many as a third of them are neutral on this issue. Over half of the respondents think that digitalization is a real threat to privacy and one-third of them are frustrated by the increased level of digitalization in their lives. However, seven out of ten respondents would use digital public services if they had access to them.

A large number of respondents are concerned about their privacy in the online environment. Thus, 34.2 percent of respondents are concerned, and 10.9 percent of respondents are extremely concerned about their privacy in the online environment (Figure 6.17). In addition, 61.8 percent of them are concerned about the excessive collection of their personal information and data on the Internet (Figure 6.18). Over half of the respondents stated that they are concerned about privacy violation when using the Internet (Figure 6.19). It is worrying that as many as 47 percent of respondents think that the existing laws are not sufficient to protect peoples' online privacy and only 14.7 percent of the respondents believe that the laws protect them (Figure 6.20). Furthermore, only 12 percent of respondents think that the government puts enough effort into ensuring that citizens are protected against online privacy violation (Figure 6.21).

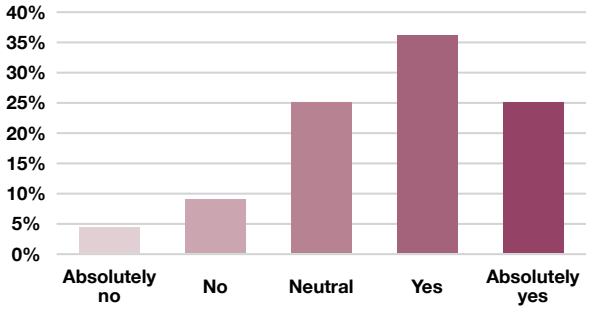
Figure 6.17. I am concerned about my online privacy.



Note: In percentage of respondents.

Source: Authors.

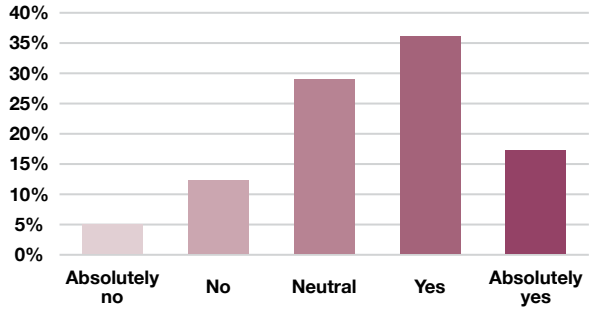
Figure 6.18. I am concerned about extensive collection of my personal information over the Internet.



Note: In percentage of respondents.

Source: Authors.

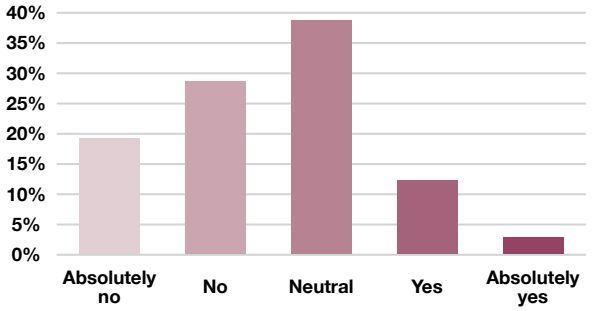
Figure 6.19. I am concerned about my privacy violation when using the Internet.



Note: In percentage of respondents.

Source: Authors.

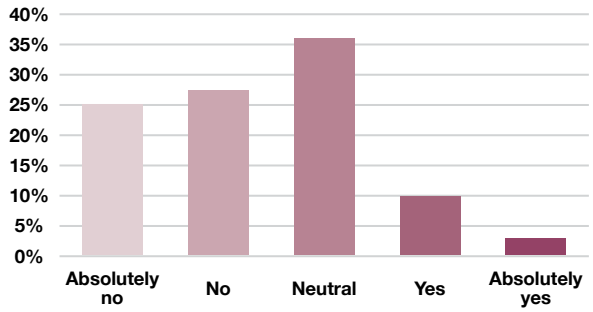
Figure 6.20. The existing laws in my country are sufficient to protect peoples' online privacy.



Note: In percentage of respondents.

Source: Authors.

Figure 6.21. The government is doing enough to ensure that citizens are protected against online privacy violation.

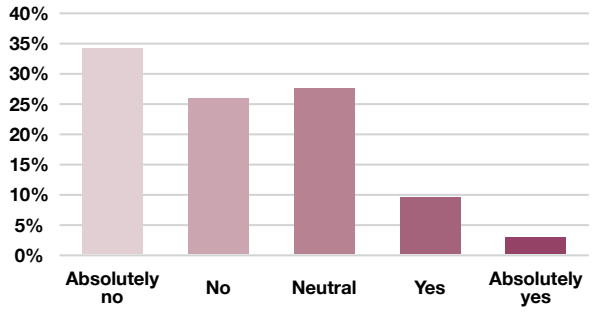


Note: In percentage of respondents.

Source: Authors.

In the survey, respondents were also asked about attitudes related to sharing private information online. The results are shown in Figures 6.22 to 6.25. People who have experienced online privacy violation incidents are generally unwilling to share private information on the Internet. As many as 59.8 percent of respondents do not agree with sharing private data on the Internet, and 59.3 percent do not consider it acceptable to publish information about their current location. 55.6 percent do not consider it acceptable to publicly disclose who they are currently spending time with, and 56.5 percent of respondents disapprove of sending credit card information when shopping online. Approximately one in five respondents has a neutral opinion on these issues. At the same time, women are less inclined to share private information than men, although most of the male respondents also have a negative attitude toward these issues.

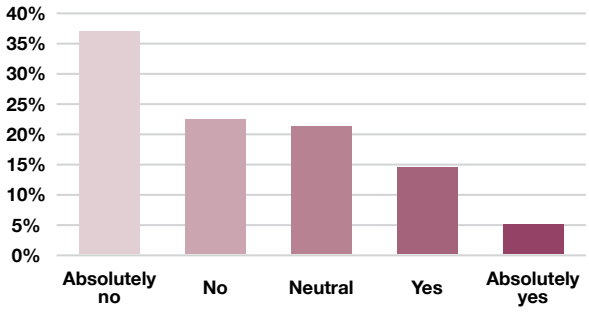
Figure 6.22. I don't mind sharing private information on the Internet.



Note: In percentage of respondents.

Source: Authors.

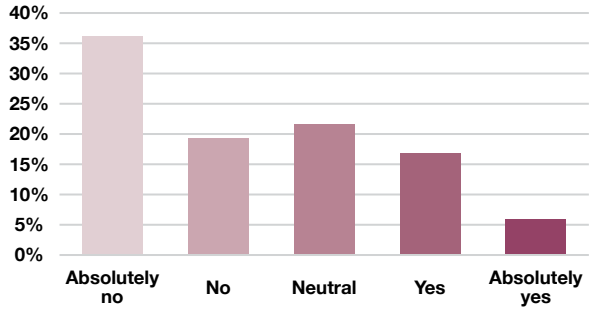
Figure 6.23. I don't mind posting my current location on the Internet.



Note: In percentage of respondents.

Source: Authors.

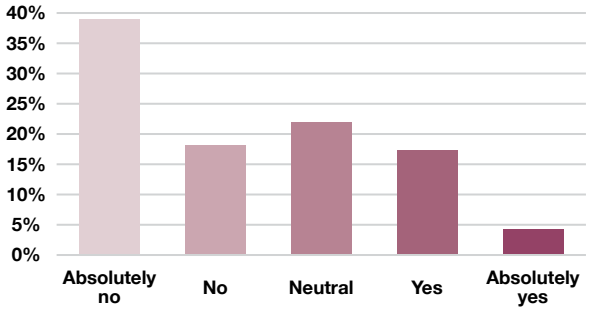
Figure 6.24. I don't mind posting with whom I am at the moment on the Internet.



Note: In percentage of respondents.

Source: Authors.

Figure 6.25. I see no problem in sending my credit card data when buying online.

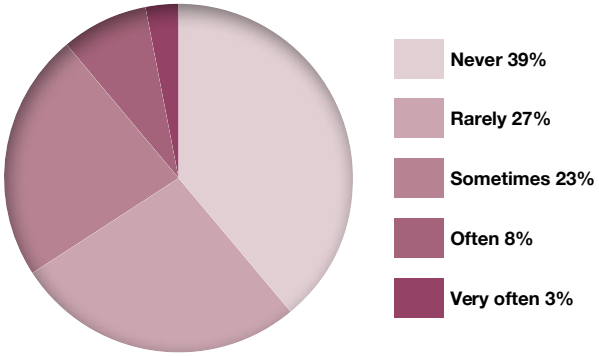


Note: In percentage of respondents.

Source: Authors.

The results of the survey, further, indicate that every tenth respondent often or very often gives fictitious responses in order to avoid giving true information about themselves (Figure 6.26). 18.7 percent of respondents sometimes, 10.3 percent often, and 4.5 percent very often use a different name or e-mail address when registering on a website without revealing their real identity (Figure 6.27). 45.8 percent of respondents often or very often fill in the data only partially when registering on a website (Figure 6.28). 13.2 percent of respondents never try to eliminate cookies that track their online activities (Figure 6.29). Nearly a quarter of respondents often or very often try to hide their identity when browsing the Internet (Figure 6.30), and 71.9 percent of respondents often or very often refuse to provide personal information to untrustworthy websites (Figure 6.31).

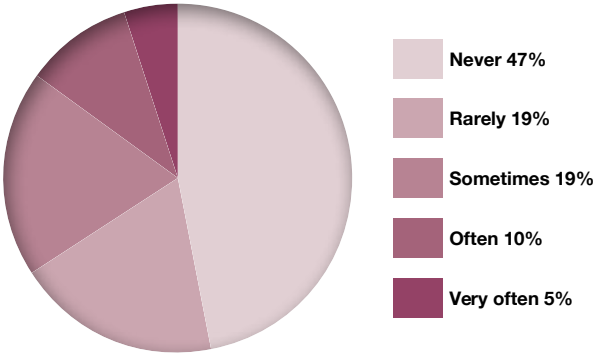
Figure 6.26. I give fictitious responses to avoid giving websites real information about myself.



Note: In percentage of respondents.

Source: Authors.

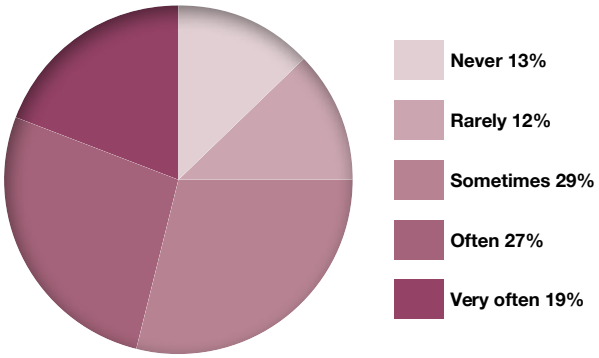
Figure 6.27. I use another name or e-mail address when registering on a website without divulging my real identity.



Note: In percentage of respondents.

Source: Authors.

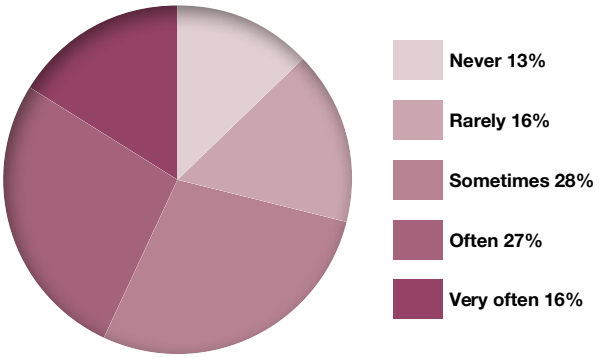
Figure 6.28. When registering on a website, I only fill in data partially.



Note: In percentage of respondents.

Source: Authors.

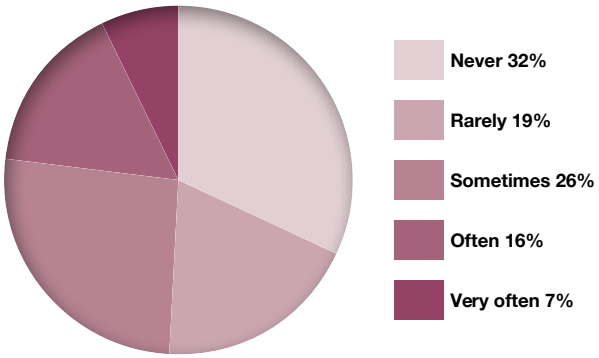
Figure 6.29. I try to eliminate cookies that track my Internet activities.



Note: In percentage of respondents.

Source: Authors.

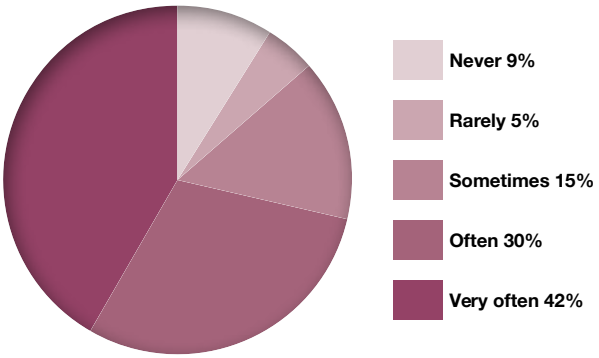
Figure 6.30. I try to disguise my identity when browsing (private browsing option).



Note: In percentage of respondents.

Source: Authors.

Figure 6.31. I refuse to provide personal information to untrustworthy websites.

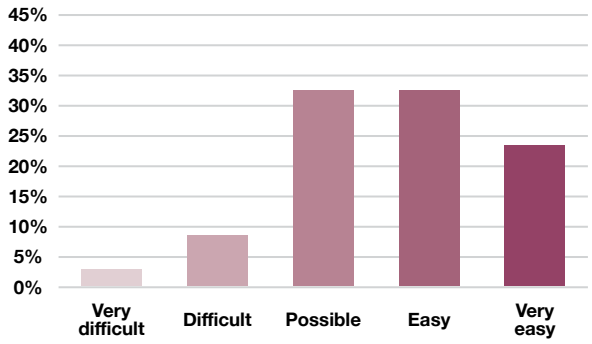


Note: In percentage of respondents.

Source: Authors.

The results of the survey indicate that the level of social support is relatively high, with a mean value of 3.7, which indicates that 88.7 percent of respondents can easily get practical help related to using the Internet from people close to them (family members or friends) (Figure 6.32).

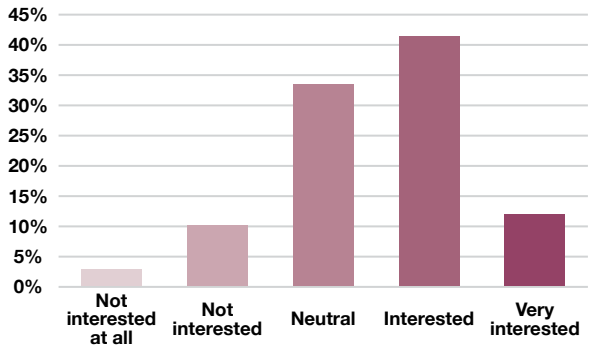
Figure 6.32. How easy can you get practical help in using the Internet from people close to you (members of your family, friends, colleagues, …) if you should need it?



Note: In percentage of respondents.

Source: Authors.

Figure 6.33. How interested would you be in using new online services/technologies immediately after they are available?



Note: In percentage of respondents.

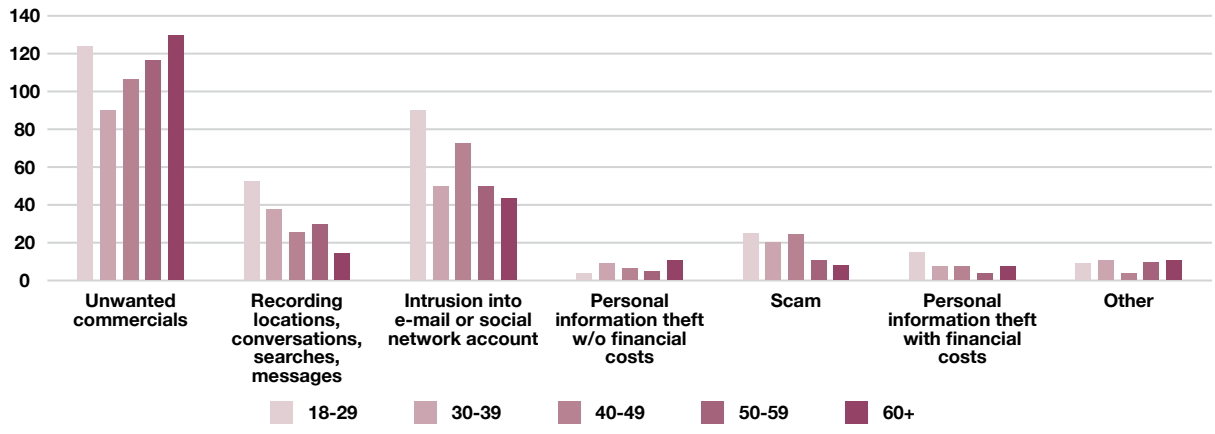
Source: Authors.

The general interest in using new online services/technologies immediately after they are available is relatively high. More than half of the respondents expressed interest in using them despite their experienced online privacy breaches, while 12.7 percent of respondents said they would not be interested in using new services or technologies.

6.1. Privacy violation online by the socio-demographic characteristics of Internet users

Subjective assessment of privacy violation online varies according to the socio-demographic characteristics of Internet users[11]. Figure 6.34 shows that unwanted commercials are perceived as privacy violations online dominantly by the oldest age groups of Internet users because the share of older respondents who consider unwanted commercials as privacy violation online is larger than the respective share of that age group in the sample. Following the same logic, recording location, conversations, etc. is viewed and experienced as an OPVI mostly by younger Internet users. Intrusion into e-mail or social network account was mostly experienced by the youngest Internet user population, probably because they use social networks more than older respondents. Here it is interesting to mention that recording locations bothers older Internet users less. Scam was reported as a privacy incident mostly by middle-aged Internet users. A worrying result was related to personal information loss with financial costs. Although this type of OPVI was reported in a small number of cases, the victims fall into the youngest group of Internet users, those 18–29 years old.

Figure 6.34. Age structure of Internet users who have experienced various types of OPVI



Note: In number of OPVI.

Source: Authors.

11 This chapter is based on the paper by Budak, Škrinjarić, and Rajh (2022).

One would assume that education level attained would play a significant role in OPVI reported. The distribution of OPVI per type is, however, distributed in line with the structure of middle-aged respondents in the sample. This means that an unexpectedly low number of incidents were reported by the less educated respondents, while the share of the highest educated Internet users who experienced theft of personal data without financial loss is above their respective share in the sample.

Unproportionally high incidences of scam and personal information theft without financial costs were reported by managers. The greatest variations compared to their relative share in the sample were observed for the respondents in the occupational category of workers, who overreported scams, recording locations, conversations, etc., and personal information theft with financial damage. On the other hand, personal information theft without financial damage in this occupation group was below its relative share in the sample. Students and retired people underreported scams.

Differences were not observed in terms of gender and household income. With regard to regional distribution, Croatian Internet users in the Pannonian region largely reported recording location, conversations, etc. as privacy incidents and had the lowest incidence of personal information theft without financial loss. In the Adriatic region, most privacy violations refer to scams and personal information theft with financial losses. Internet users in the capital city of Zagreb have fewer complaints about scams, close to the respondents from Northern Croatia who have a very low report rate of personal information theft without financial costs. In smaller settlements with less than 50,000 inhabitants, the types of privacy incidents reported are in line with the share of such settlements in the total sample. The urban/rural deviations are observed as larger share of personal information theft without financial costs in towns up to 100,000 inhabitants and in large cities where scams and recording location, conversations, etc., are reported more frequently.

6.2. Profiles of Internet users resilient to privacy violation online

Having gained insight into the real experience with privacy violation online and opinions of Internet users, the central question is how individuals cope with the OPVI. Figure 6.35 presents responses to the adapted Smith et al. (2008) short measure of resilience scale (the Brief Resilience Scale, BRS). We kept the reversed statements for methodological reasons and answers were given on a five-point Likert scale from 1 – Strongly disagree to 5 – Strongly agree.

Figure 6.35. Resilience of Internet users to privacy violation online

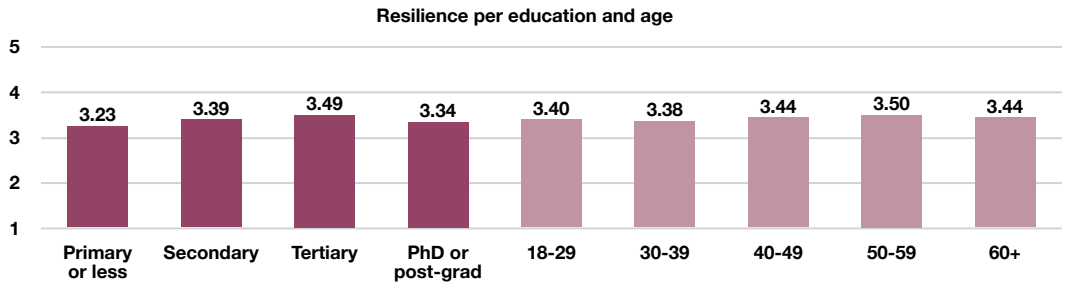
Source: Authors.

Internet users on average recover quickly after the online privacy violation incident, and this is an expected behavior given that the prevalent cases are unwanted commercials/ recording location, i.e., privacy violation rated by its victims as low severity incidents. Time of recovery is only one component of measuring resilience, and adaptive capacity is another one. Internet users did not have much trouble coming through their most recent privacy violation incident (3.55 score on a scale of 1 to 5).

However, some differences among respondents were observed according to their socio-demographic characteristics. As for the privacy violation experience, there were negligible

variations of resilience among men and women (average score of 3.41 and 3.45, respectively). One would expect younger people to be more resilient to privacy incidents, yet this is not the case since all ages have a similar resilience score of about 3.4. The 50 to 59 age group appears to be slightly more resilient. Respondents with low level of education attained are less resilient compared to Internet users with higher education (Figure 6.36).

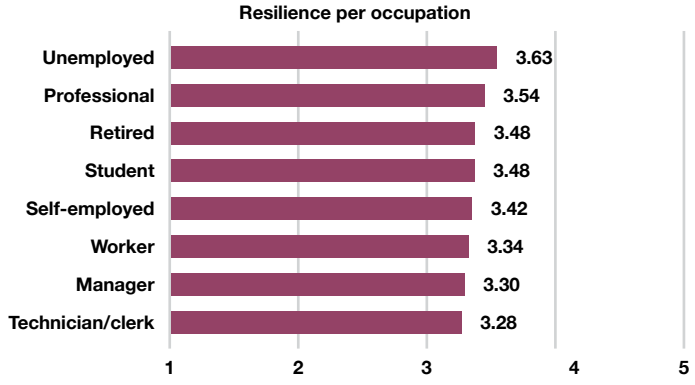
Figure 6.36. Resilience to OPVI per educational and age structure of Internet users



Source: Authors.

Internet users with primary or lower education showed to be less resilient to privacy incidents they have experienced online, and unemployed respondents exhibited more resilience (3.63) compared to other occupational categories of Internet users (Figure 6.37). Among the less resilient occupations stand technicians/clerks and managers (score of 3.3 and less).

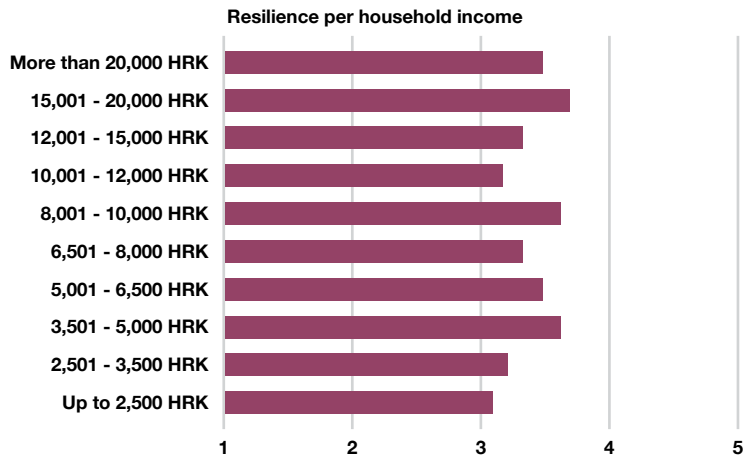
Figure 6.37. Resilience to OPVI per occupation of Internet users



Source: Authors.

No conclusive variations were observed among different categories of Internet users grouped by household income (Figure 6.38).

Figure 6.38. Resilience to OPVI per Internet users' household income

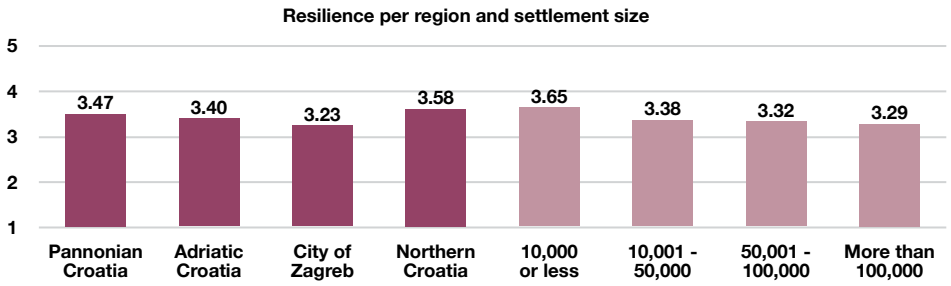


Note: As of January 1, 2023, Croatia adopted the euro as its official currency with the official fixed exchange rate 1 EUR = 7.53450 HRK.

Source: Authors.

Regional variations and observed differences between urban and rural areas are presented in Figure 6.39. More resilient Internet users live in the northern part of Croatia and in smaller settlements.

Figure 6.39. Resilience to OPVI by region and settlement size



Source: Authors.

It is evident that Internet users in Croatia consider unwanted commercials and recording locations, conversations, messages, and searches as the main types of OPVI. Unwanted commercials are experienced more by older Internet users, while recording locations, conversations, messages, and searches is perceived as an online privacy violation dominantly by the youngest age group. The younger Internet users, who are so-called "digital natives", are more likely than other Internet users to be the victims of personal information theft with financial loss. This might be simply because this group is more exposed to the risk (e.g., they do more online shopping or e-banking activities). In general, privacy violations with severe consequences for young Internet users underscore the worrying finding of their lack of cautiousness in online transactions. As far as resilience is concerned, the Internet user's age does not make a difference, except for a slightly higher resilience in the group aged 50 to 59 years.

Another interesting finding is that less educated Internet users report less online privacy violations but also showed to be less resilient when compared to better educated Internet users. With regard to occupation, managers reported a high incidence of scams and personal information theft without financial loss, but at the same time, showed to be less resilient. Unemployed Internet users are more resilient as well as those living in Northern Croatia and in smaller settlements.

Gender and income of Internet users make no difference in reporting privacy violation incidents and negligible differences were observed in the level of resilience demonstrated. This might indicate that some other explanatory factors are in play, such as personality traits and other personal attributes, using the Internet for specific activities (for private or business purposes), or the level of Internet skills.

Most online privacy violation problems arise from insufficient education regarding online privacy and from lacking digital competences when using various digital services. This is particularly evident from the fact that most of these subjectively reported privacy violation cases are not considered a "real" violation of online privacy in the legal sense. As for digital

competences, most of these privacy violation cases can be significantly reduced by simply changing the settings (usually the privacy settings) on electronic devices and paying more attention to accepting various "cookies" when browsing the Internet. However, although this is the most common form of violation of their privacy, Croatian Internet users are also aware that these are not so serious violations of privacy, compared to those where personal data are stolen or someone hacks into e-mail or social media accounts.

Finally, in terms of reaction to the subjectively experienced privacy violation online, an average Internet user recovers rather fast. However, there are some differences in the level of resilience among different socio-demographic groups and it can be concluded that socio-demographic variables affect, to a certain degree, resilience to online privacy violation. Therefore, socio-demographic variables should be included in any theoretical model of antecedents of resilience to online privacy violations and more detailed analyses of the typology performed. Before modelling resilience to OPVI, the psychometric adequacy of main measurement scales needs to be confirmed.

6.3. Psychometric characteristics of the resilience measurement scale

The aim of this chapter is to test the measurement scale for measuring the resilience to OPVI[12]. As resilience is at the core of the REPRICON research, before proceeding to modelling and other in-depth analyses, the psychometric adequacy of the measurement scale must be confirmed by assessing its reliability, convergent validity, and dimensionality. The Cronbach alpha coefficient analysis was applied, as well as explorative and confirmative factor analysis.

Reliability of scales is analyzed with Cronbach's alpha coefficients, alpha-if-deleted indicators, and correlation analysis. Cronbach's alpha coefficients indicate the scale's internal consistency, i.e., to what extent are items from the same scale correlated as a group. The

12 This chapter is based on the paper by Rajh, Škrinjarić, and Budak (2021).

higher the value of Cronbach's alpha coefficient (range is between 0 and 1), the more each item shares covariance and the probability is higher that items measure the same underlying concept, i.e., the same latent variable. The "good" CA coefficient should be at least 0.65–0.8, and scores below 0.5 are generally not acceptable, in particular for one-dimensional scales (Kline, 1998).

Item-test correlation indicates how strong the correlation is between every single item in relation to the rest of the items in the scale. The greater the value of the coefficient, the stronger the correlation is between the item and the total scale.

Alpha-if-deleted is used for measuring the internal consistency of the scale. It indicates the change in Cronbach's alpha if each respective item is removed from the scale. If the item removal results in increased Cronbach's alpha, the exclusion of that particular item from the measurement scale is advised.

However, a high value of CA coefficient does not mean that the measurement scale is one-dimensional. The dimensionality of the scale is tested by exploratory and confirmatory factor analyses with measurement models where each manifest variable only loads on one latent variable, and with the assumption of the independence of measurement errors (Gerbing & Anderson, 1988; Kline, 1998).

Cronbach alpha coefficient of 0.8961 and results of reliability analysis (Table 6.4) indicate that the measurement scale for resilience index (RES) has an acceptable level of reliability.

Table 6.4. Reliability assessment

Item	Inter-item correlation	Item-test correlation	Alpha-if-deleted
res_1	0.6101	0.6623	0.8867
res_2	0.5828	0.7398	0.8748
res_3	0.6129	0.6543	0.8879
res_4	0.5746	0.7637	0.8710
res_5	0.5799	0.7484	0.8734
res_6	0.5787	0.7516	0.8729

Source: Authors.

Exploratory factor analysis (EFA) is a measurement technique used to examine structural relations among variables. It is used when both observed and latent variables are assumed to be measured at the interval level to assess the scale's convergent validity and for preliminary testing of the scale's dimensionality. One factor was extracted with the principal component method. The Kaiser-Guttman rule was applied as the criterion for number of factors extracted. The Kaiser-Guttman rule specifies that factors with eigenvalues greater than 1 are retained. Table 6.5(A) shows the resulting factor structure. One-factor solution explains 95.58 percent of variance.

Table 6.5. Exploratory factor analysis results

Panel A: Eigenvalue

Factor	Eigenvalue	Cumulative eigenvalue	Explained variance	Cumulative explained variance
1	3.58725	3.58725	0.9558	0.9558
2	0.26637	3.85362	0.0710	1.0268
3	0.21071	4.06433	0.0561	1.0830
4	0.03067	4.09500	0.0082	1.0911
5	-0.15839	3.93661	-0.0422	1.0489
6	-0.18359	3.75302	-0.0489	1

Panel B: Eigenvector

Item	Factor 1
res_1	0.7095
res_2	0.7874
res_3	0.7056
res_4	0.8115
res_5	0.8031
res_6	0.8139

Source: Authors.

Exploratory factor analysis results indicate that the tested scale is unidimensional and that it has exhibited convergent validity. Therefore, the set of six items can be observed as a single measurement scale for measuring perceived consumer privacy resilience in an online setting.

Convergent validity will also be further explored with confirmatory factor analysis. Confirmatory factor analysis (CFA) is a multivariate statistical procedure that is used to test how well the measured variables represent the number of constructs. Confirmatory factor analysis therefore is used to test the assumed relations among manifest and latent variables (Hair, Black, Babin, Anderson, & Tatham, 2006; Kline, 1998) and it is considered a more rigorous test of convergent validity (Yoo, Donthu, & Lee, 2000).

The measurement model was tested with the assumption that the scale is one-dimensional. Three separate models were tested (Table 6.6). Model 1 includes all items into the model; Model 2 includes only items with correct direction (items res_1, res_3, and res_5); Model 3 is the same as Model 2, but it is tested only on a sample of respondents younger than 60 years.

Table 6.6. Confirmatory factor analysis results

	Model 1	Model 2	Model 3
res_1			
Factor1	0.694*** (0.019)	0.662*** (0.024)	0.691*** (0.025)
Constant	2.398*** (0.062)	2.398*** (0.062)	2.359*** (0.068)
res_2			
Factor1	0.774*** (0.015)		
Constant	2.786*** (0.070)		
res_3			
Factor1	0.695*** (0.019)	0.714*** (0.023)	0.743*** (0.024)
Constant	2.735*** (0.069)	2.735*** (0.069)	2.753*** (0.077)
res_4			
Factor1	0.807*** (0.014)		
Constant	3.034*** (0.075)		
res_5			
Factor1	0.809*** (0.014)	0.820*** (0.022)	0.823*** (0.022)
Constant	3.051*** (0.075)	3.051*** (0.075)	2.991*** (0.082)
res_6			
Factor1	0.828*** (0.013)		
Constant	3.121*** (0.077)		
Number of items	6	3	3
N	1,000	1,000	810
$\chi 2$	593.91***	823.40***	750.09***
RMSEA	0.255	0.000	0.000
GFI	0.842	1.000	1.000
CFI	0.844	1.000	1.000
CR	0.896	0.776	0.796
AVE	0.592	0.541	0.569

Notes: *** denotes significance level at $p < 0.01$. Abbreviations: RMSEA – root mean square error of approximation, GFI – goodness of fit index, CFI – comparative fit index, CR – Raykov's factor reliability coefficient, AVE – average variance extracted.

Source: Authors.

Fit indices indicate a somewhat lower fit for Model 1 (relatively high value of RMSEA and low value of CFI). Results for Model 2 and Model 3 indicate a better fit to empirical data. Cronbach's alpha values for the shortened scale are 0.7747 and 0.7955 and indicate an acceptable level of reliability for the shortened scale.

Confirmatory factor analysis results indicate that all factor loadings are statistically significant, and it can be concluded that the tested scale has an acceptable level of convergent validity. The results also indicate that the scale is one-dimensional.

The results indicate that the measurement scale has satisfactory psychometric characteristics. The measurement scale possesses characteristics of reliability, convergent and discriminant validity, and its dimensionality fits the conceptualized dimensionality.

6.4. Psychometric characteristics of self-efficacy and optimism and pessimism measurement scales

Next the psychometric characteristics of three adapted scales were assessed to test their applicability in explaining the level of resilience after the online privacy violation incident[13]. These are self-efficacy, optimism, and pessimism scales. As described in Chapter 5.3, the self-efficacy variable (SEF) is assessed by using the generalized self-efficacy (GEF) scale from Schwarzer et al. (1997). Since the original scale is adapted for the REPRICON research purpose, this methodological change in the adapted scales needs to be validated.

In the original GEF scale, ten items are evaluated by a four-point Likert scale ranging from 1 – Not at all true, 2 – Barely true, 3 – Moderately true, to 4 – Exactly true (Schwarzer et al., 1997). To measure self-efficacy (SEF) in the resilience to privacy violation online survey, the original GEF scale has been adapted by shortening it to four items (Table 6.7).

To measure optimism (OPT) and pessimism (PES) variables, we have adapted the original O-P scale (Chang et al., 1997) by shortening the number of items. Three items from the original optimism scale (opt 1–3) and three items from the original pessimism scale (pes 1–3) were used in the questionnaire, as shown in Table 6.7.

13 Based on the paper by Škrinjarić, Budak, and Rajh (2021).

Table 6.7. Description of items used to build latent constructs

Latent construct	Item	Description
Self-efficacy (SEF)	sef_1	It is easy for me to stick to my aims and accomplish my goals.
	sef_2	Thanks to my resourcefulness, I know how to handle unforeseen situations.
	sef_3	I can solve most problems if I invest the necessary effort.
	sef_4	I can remain calm when facing difficulties because I can rely on my coping abilities.
Optimism (OPT)	opt_1	I always look on the bright side of things.
	opt_2	I'm always optimistic about my future.
	opt_3	In general, things turn out all right in the end.
Pessimism (PES)	pes_1	Rarely do I expect good things to happen.
	pes_2	Things never work out the way I want them to.
	pes_3	Better to expect defeat: then it doesn't hit so hard when it comes.

Source: Authors.

Answers to what extent the respondent agrees with the statements shown in Table 6.7 were given on a five-point Likert scale ranging from 1 – Absolutely no, 2 – No, 3 – Neutral, 4 – Yes, to 5 – Absolutely yes.

The reliability of the measurement scale is analyzed by Cronbach alpha coefficient (CA), alpha-if-deleted indicator, and a range of correlation analyses. CA coefficient is used as a measure of scale reliability because it measures internal consistency, as explained in Chapter 6.3. Cronbach's alpha coefficient values for optimism, pessimism, and self-efficacy, respectively, and other correlation coefficients in Table 6.8 indicate that the measurement scales used to measure latent constructs possess a satisfactory level of reliability. Both analyzed types of correlations indicate a high degree of correlation of each statement with the overall measurement scale, while alpha-if-deleted values indicate that in this case the removal of any statement would cause a decrease in CA coefficient, i.e., the scale would become less reliable. This is an argument for keeping all current items on the scale.

Table 6.8. Item correlations and Cronbach alphas

Latent construct	Item	Inter-item correlation	Item-rest correlation	Cronbach alpha	Alpha-if-deleted
Optimism	opt_1	0.5329	0.6801	0.8021	0.6953
	opt_2	0.4893	0.7151		0.6571
	opt_3	0.7013	0.5541		0.7944
Pessimism	pes_1	0.5062	0.6877	0.7971	0.6721
	pes_2	0.5976	0.6166		0.7481
	pes_3	0.5961	0.6178		0.7469
Self-efficacy	sef_1	0.5234	0.5441	0.7912	0.7672
	sef_2	0.4644	0.6341		0.7223
	sef_3	0.4872	0.5987		0.7402
	sef_4	0.4707	0.6242		0.7273

Source: Authors.

Exploratory factor analysis (EFA) was conducted to test convergent validity of measurement scales, as well as to preliminary test their dimensionality. Table 6.9(A) shows EFA results.

Table 6.9. Exploratory factor analysis results

Panel A: Eigenvalues

Factor	Eigenvalue	Cumulative eigenvalue	Percentage of explained variance	Cumulative percentage of explained variance
1	3.8252	3.8252	0.8458	0.8458
2	1.2588	5.0840	0.2783	1.1241
3	0.1278	5.2118	0.0283	1.1523
4	0.0160	5.2278	0.0035	1.1559
5	-0.0432	5.1846	-0.0095	1.1463
6	-0.0798	5.1048	-0.0176	1.1287
7	-0.1227	4.9822	-0.0271	1.1016
8	-0.1337	4.8484	-0.0296	1.0720
9	-0.1527	4.6957	-0.0338	1.0382
10	-0.1729	4.5228	-0.0382	1.0000

Panel B: Eigenvectors

Latent construct	Item	F1	F2	F3
Optimism (OPT)	opt_1	0.7312		
	opt_2	0.7322		
	opt_3	0.5706		
Pessimism (PES)	pes_1	-0.7962		
	pes_2	-0.6553		
	pes_3	-0.7055		
Self-efficacy (SEF)	sef_1		0.5985	
	sef_2		0.7032	
	sef_3		0.6502	
	sef_4		0.6814	

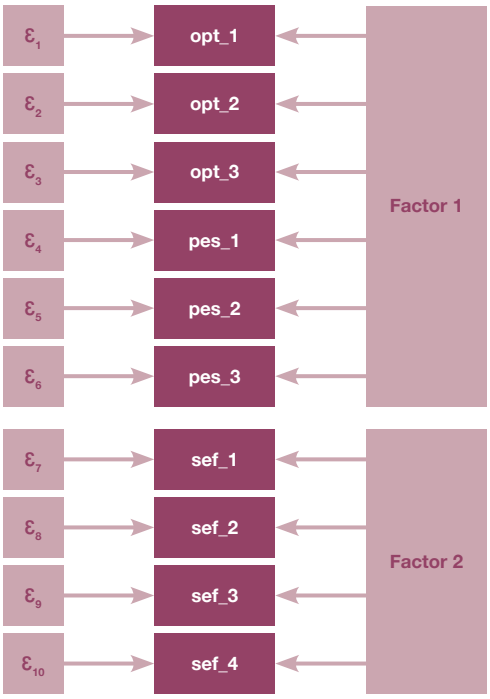
Note: Principal factor method was used, and factors were rotated using orthogonal varimax rotation.

Source: Authors.

EFA results indicate that the SEF measurement scale is unidimensional. All SEF items have high factor loadings on their respective factor, as shown in Table 6.9(B). EFA results also indicate that the SEF scale poses the attribute of convergent validity. Therefore, the initial set of four SEF items can be considered as one measurement scale for measuring self-efficacy. Empirical evidence does not support the theoretical notion of OPT and PES as two separate measurement scales, but rather as opposite poles of the same measurement scale.

Convergent validity was also assessed with confirmatory factor analysis, with two latent variables (constructs), one for SEF, and another for PES and OPT as elements of one measurement scale (Figure 6.40).

Figure 6.40. Confirmatory factor analysis model structure



Source: Authors.

Fit indices indicate an acceptable level of fit of measurement model to empirical data. CFA results further confirm EFA results (Table 6.10). All analyzed items load on their respective factors and all loadings are statistically significant. Both SEF scale and combined OPT-PES scale have acceptable levels of convergent and discriminant validity. Results also indicate that both scales are unidimensional.

Table 6.10. Confirmatory factor analysis results

Item	Factor	Model estimates
opt_1	Factor1	1.000 (.)
opt_2	Factor1	1.038*** (0.038)
opt_3	Factor1	0.764*** (0.037)
pes_1	Factor1	-1.226*** (0.050)
pes_2	Factor1	-0.935*** (0.046)
pes_3	Factor1	-1.046*** (0.049)
sef_1	Factor2	1.000 (.)
sef_2	Factor2	1.143*** (0.067)
sef_3	Factor2	1.039*** (0.062)
sef_4	Factor2	1.179*** (0.069)
N		1,000
$\chi 2$ statistic		292.17***
RMSEA		0.087
GFI		0.929
CFI		0.936

Notes: *** denotes significance level at $p < 0.01$. Abbreviations: RMSEA – root mean square error of approximation, GFI – goodness of fit index, CFI – comparative fit index.

Source: Authors.

Conclusively, empirical results indicate that both SEF scale and combined OPT-PES scale exhibit an acceptable level of reliability, as well as convergent and discriminant validity. The dimensionality of the SEF scale is in accordance with the literature. The OPT-PES scale is a unidimensional scale with OPT and PES as opposite poles of one scale, rather than two separate scales.

The basic descriptive statistics of the survey data and testing the scales employed in the questionnaire facilitated the next phase of the research: exploring the resilience of Croatian consumers to online privacy violation.

7. Croatian consumers' resilience to online privacy violation

The empirical data collected allowed us to develop the typology of Croatian consumers regarding their resilience to online privacy violations as well as the change in their attitudes after the incident.

7.1. Typology of consumers

In this chapter, we examine if consumers who had recently experienced an OPVI can be segmented into distinct groups based on their resilience to online privacy violation (RES) and what the common characteristics are among members of each cluster[14].

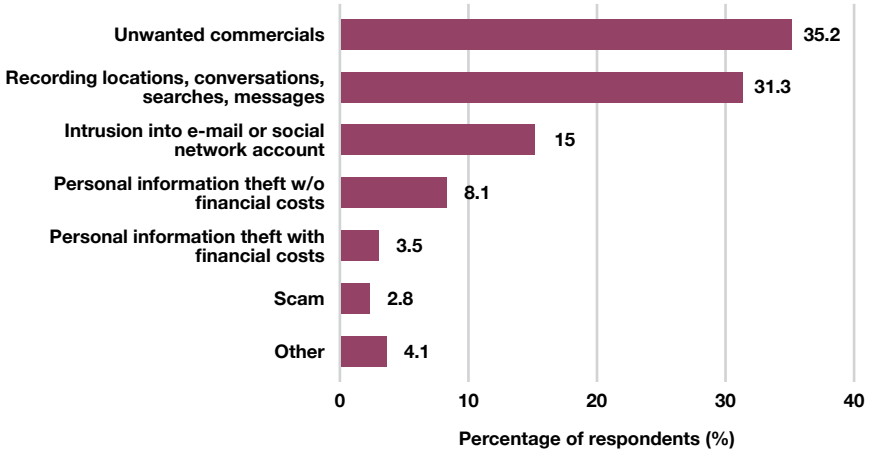
We again employed the exploratory and confirmatory factor analysis techniques, calculated Cronbach's alpha and alpha-if-deleted coefficients, and proceeded with the K-means cluster analysis. The differences among the groups of respondents were tested using the chi-square test and ANOVA.

Latent constructs in our analysis include resilience to online privacy concern (RES), online privacy concern (OPC), online privacy awareness (OAW), Internet benefits (BNF), digitalization anxiety (DA), and protective behavior (PB). Items used to build the latent constructs can be found in the questionnaire (Appendix 3). We introduced two single items in the analysis: general Internet attitude (GIAS) and privacy violation seriousness (PV_ser). PV_ser is measured by assessing subjective evaluation of how severe the experienced privacy incident was for the respondent, ranging from 1 - Negligibly serious to 5 - Very serious.

Answers to an open-ended question about OPVI were grouped into six categories of online privacy violation cases (Figure 7.1). Unwanted ads and recording one's location, conversations, Internet searches, and messages were the most common OPVIs reported, but the least harmful ones as well (Figure 7.2).

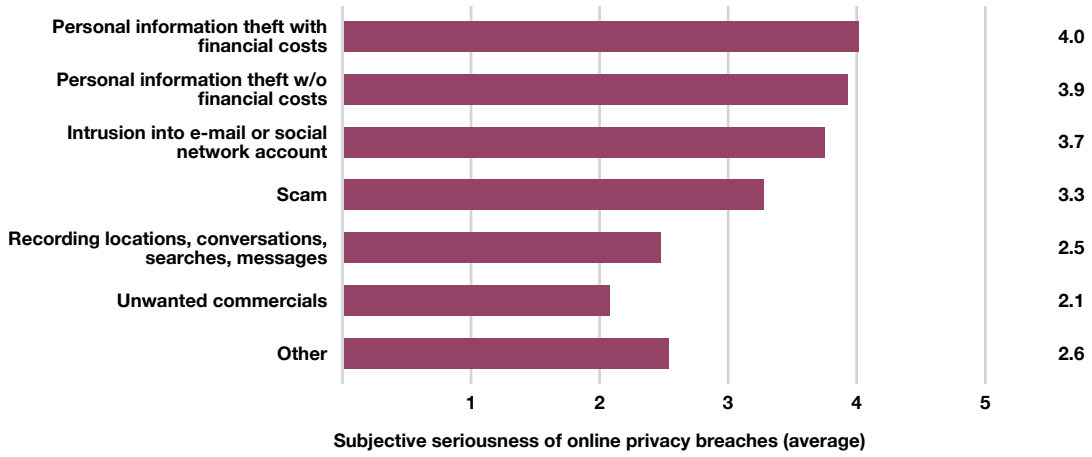
14 This chapter is based on Budak, Rajh and Škrinjarić (2023).

Figure 7.1. Online privacy violation cases



Source: Authors.

Figure 7.2. Perceived severity of online privacy violations

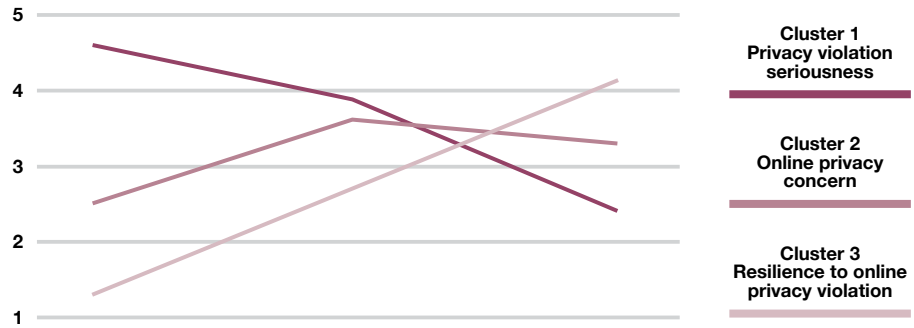


Note: 1 - Negligibly serious; 5 - Very serious.

Source: Authors.

K-means cluster analysis was employed to classify consumers based on three online privacy related variables: PV_ser, OPC, and RES. Results of the K-means cluster analysis differentiated three homogeneous segments of Internet users (Figure 7.3).

Figure 7.3. K-means cluster analysis results



Source: Authors.

Cluster 1 is comprised mainly of younger Internet users with low resilience and high level of privacy concern. Also, they exhibit the highest perceived seriousness of their experienced OPVI.

Members of Cluster 2 exhibit moderate levels of resilience and a negative attitude toward the Internet. Their perceived seriousness of experienced OPVI is at lower levels. However, they are still actively involved in online shopping. The age profile of this cluster mainly corresponds to the average of the entire sample.

Respondents from Cluster 3 demonstrate the highest level of resilience, but also their OPVIs are perceived as the least serious. Cluster members are also characterized by low levels of privacy concern and digitalization anxiety, as well as positive attitudes toward the Internet. This cluster is comprised of a larger share of older Internet users.

The findings on the typology of Internet users who experienced OPVI differentiated three groups of Internet users, i.e., consumers (low-resilience, moderate-resilience, and high-resilience). A set of antecedents and factors influencing the resilience to OPVI is further analyzed in the subsequent chapters.

7.2. Internet literacy and resilience to online privacy violation

An Internet user who possesses advanced Internet skills might react differently to privacy breaches online[15]. The literature indicates that there is a link between the level of digital literacy and resilience. Previous research has mostly focused on studying OPVI on social networks (Chen & Chen, 2015; Feng & Xie, 2014), especially among young users. Tran et al. (2020) use a sample of Vietnamese students and show that as students are digitally literate, they are more likely to be digitally resilient. Internet users with insufficiently developed digital competences are especially susceptible to OPVI (Smith, Hewitt, & Skrbiš, 2015).

However, as the Internet is currently available to more than 80 percent of the population in developed countries (International Telecommunication Union, 2015), this research focuses on the general public and focuses on the effect of Internet skills and range of activities performed online on resilience to OPVI. A special contribution of the research is that it uses a nationally representative sample of Internet users from 2021, which is not biased with regard to Internet skills or privacy attitudes.

The central variable in the model is the individuals' resilience to OPVI (RES). Internet skills (SKILL) and the type of Internet service or activity used (WEB) can significantly determine the level of resilience to online privacy violations (Tran et al., 2020; Smith et al., 2015). Frequent and advanced Internet users, on the one hand, may be more aware of the risk of privacy violations in the online environment and therefore may be more resilient; but on the other hand, such Internet users may be so addicted to the Internet that they simply do not feel any concern for the violation of their privacy, and, as such, are less resilient to online privacy breaches.

Online privacy concern (OPC) involves the rights of an individual concerning the storing, reusing, and provision of personal information to third parties and displaying of information pertaining to oneself on the Internet (Malhotra et al., 2004). Research done by Ginosar and Ariel (2017) points to three separate domains of OPC: (1) user privacy concerns and behavior,

15 This chapter is based on Škrinjarić (2023).

(2) website privacy notices and practices, and (3) state privacy policies and regulations. Individuals, i.e., Internet users, vary in their privacy concerns about collection, sharing, and unauthorized manipulation of their personal sensitive information and their resilience will depend on this concern.

The model was also extended with a measure of digital anxiety (DA), which is defined as a fear of computers and technology in general. DA leads to an increased level of concern for privacy in the online environment (Stewart & Segars, 2002) and individuals suffering from DA are thus speculated to have lower levels of RES.

Social support (SS) refers to the number of close confidants, the sense of concern from other people, and the relationship with neighbors, with a focus on the accessibility of practical help in recovery.

Individuals can also take certain steps to increase their resilience to OPVI, i.e., they can adopt certain types of protective behavior (PB) (Lwin et al., 2007).

Personality traits (PT) can be defined as “the substance of personality” ”(McCrae & Costa, 1987), an individual’s tendencies resulting in different attitudinal and behavioral patterns across a diverse set of situations. Thus, depending on their personality, individuals’ opinions and actions regarding resilience to OPVI differ. The upside of personality traits in explaining resilience to OPVI is their hereditary origin (Bergeman et al., 1993), as well as their stability across an individual’s lifetime (McCrae & Costa, 1987) and across cultures (Salgado, Moscoso, & Lado, 2003). Personality traits were measured using the Big Five framework (Tupes & Christal, 1992), which divides personality into five traits: (1) openness (to experience), (2) conscientiousness, (3) extraversion, (4) agreeableness, and (5) neuroticism (emotional instability).

The conceptual framework was tested using the following empirical model:

$$RES_i = \alpha + \beta_1 SKILL_i + \beta_2 WEB_i + \beta_3 OPC_i + \beta_4 DA_i + \beta_5 SS_i + \beta_6 PB_i + \delta' PT_i + \gamma' X_i + \varepsilon_i$$

where resilience to OPVI (RES) is the dependent variable, SKILL is an approximation of the respondent's skills on the Internet, WEB is the range of activities the respondent performs on the Internet, OPC is online privacy concern, DA is digital anxiety, SS is the social support that the respondent receives from their environment, PB is protective behavior on the Internet, PT is the matrix of respondents' personality traits (extraversion, agreeableness, conscientiousness, neuroticism, and openness), and X is the matrix of other respondents' socio-demographic characteristics (gender, age, education, household size, household income, occupation, settlement size, region). The REPRICON survey data were used in the empirical analysis. All latent variables (SKILL, WEB, OPC, DA, PB, PT) enter the equation in their standardized form with a zero mean and unit standard deviation and are hence interpreted in units of standard deviations from the average. A description of all items used to estimate latent variables is presented in Table 7.1.

Table 7.1. Latent variables estimation

Latent construct	Item	Description	Mean	St. dev.
Resilience to online privacy violation (RES)	res_1	I bounced back quickly after the most recent online privacy violation incident.	2.93	1.22
	res_2	It didn't take me long to recover from the most recent online privacy violation incident.	3.32	1.21
	res_3	I came through the most recent online privacy violation incident with little trouble.	2.24	1.21
Internet skills (SKILL)	skill_1	I can use a browser (e.g., Chrome, Firefox, Safari) to navigate the Internet.	4.39	0.91
	skill_2	I can register a new e-mail address (e.g., Gmail) or social network (e.g., Facebook) account.	4.26	1.05
	skill_3	I can work with/edit bookmarks.	3.85	1.35
	skill_4	I can save content from websites to my device.	3.71	1.39
Internet activities (WEB)	web_1	Receiving and sending e-mails	4.01	1.04
	web_2	Using chat/instant message services (e.g., Messenger, WhatsApp, Viber)	4.13	1.05
	web_3	Downloading music and/or movies	2.45	1.23
	web_4	Playing online games	2.34	1.34
	web_5	Paying bills/e-banking	3.18	1.41
	web_6	Attending courses online	2.32	1.41
	web_7	Online shopping	2.50	1.28
	web_8	Live streaming and/or watching multimedia content (e.g., YouTube, online radio)	3.44	1.19
	web_9	Making audio/video calls and/or meetings (e.g., Skype, Zoom)	2.86	1.27
	web_10	Using social networks (e.g., Facebook, Twitter, Instagram, TikTok)	3.65	1.34
	web_11	Following daily news online	3.75	1.05
	web_12	Using search engines to find information (e.g., Google)	4.30	0.84
	web_13	Searching for maps and driving directions	2.87	1.15
	web_14	Using online forums	2.01	1.10
	web_15	Using public services available online (e.g., e-građani, filing taxes online, e-upisi, e-dnevnik)	2.76	1.24
Personality traits – extraversion (EX)	ex_1	I see myself as someone who is reserved.	2.57	1.01
	ex_2	I see myself as someone who is outgoing, sociable.	3.97	0.92
Personality traits – agreeableness (AG)	ag_1	I see myself as someone who is generally trusting.	3.55	0.83
	ag_2	I see myself as someone who tends to find fault with others.	1.91	0.92
Personality traits – conscientiousness (CO)	co_1	I see myself as someone who tends to be lazy.	2.08	1.04
	co_2	I see myself as someone who does a thorough job.	3.95	0.84
Personality traits – neuroticism (NE)	ne_1	I see myself as someone who is relaxed and handles stress well.	3.41	0.99
	ne_2	I see myself as someone who gets nervous easily.	2.55	1.07
Personality traits – openness (OP)	op_1	I see myself as someone who has artistic interests.	3.36	1.20
	op_2	I see myself as someone who has an active imagination.	3.35	1.17

Latent construct	Item	Description	Mean	St. dev.
Digital anxiety (DA)	da_1	Digitalization is a real threat to privacy.	3.45	1.09
	da_2	I am easily frustrated by increased digitalization in my life.	2.99	1.15
Online privacy concern (OPC)	opc_1	I am concerned about my online privacy.	3.31	1.03
	opc_2	I am concerned about extensive collection of my personal information over the Internet.	3.69	1.08
	opc_3	I am concerned about my privacy violation when using the Internet.	3.50	1.07
Protective behavior (PB)	pb_1	I give fictitious responses to avoid giving websites real information about myself.	2.08	1.09
	pb_2	I use another name or e-mail address when registering on a website without divulging my real identity.	2.05	1.22
	pb_3	When registering on a website, if possible, I only fill in data partially.	3.27	1.27
	pb_4	I try to eliminate cookies that track my Internet activities.	3.17	1.25
	pb_5	I try to disguise my identity when browsing (private browsing option).	2.49	1.29
	pb_6	I refuse to provide personal information to untrustworthy websites.	3.91	1.25

Source: Authors.

First, reliability of items and psychometric properties of estimated latent constructs is analyzed (Table 7.2).

Table 7.2. Properties of latent constructs

Latent construct	Item	Loading	CA	DG	CR	AVE
Resilience to online privacy violation (RES)	res_1	0.831***	0.776	0.869	0.787	0.689
	res_2	0.798***				
	res_3	0.861***				
Internet skills (SKILL)	skill_1	0.954***	0.939	0.949	0.876	0.824
	skill_2	0.971***				
	skill_3	0.871***				
	skill_4	0.828***				
Internet activities (WEB)	web_1	0.624***	0.828	0.723	0.579	0.707
	web_2	0.556***				
	web_3	0.008***				
	web_4	-0.136***				
	web_5	0.575***				
	web_6	0.279***				
	web_7	0.685***				
	web_8	0.412***				
	web_9	0.329***				
	web_10	0.384***				
	web_12	0.488***				
	web_13	0.655***				
	web_14	0.085***				
	web_15	0.456***				
Personality traits – extraversion (EX)	ex1	-0.011	0.718	0.355	0.725	0.749
	ex2	-0.835***				
Personality traits – agreeableness (AG)	ag1	0.858***	0.478	0.791	0.795	0.655
	ag2	0.757***				
Personality traits – conscientiousness (CO)	co1	0.613***	0.655	0.798	0.844	0.676
	co2	0.989***				
Personality traits – neuroticism (NE)	ne1	-0.159***	0.718	0.183	0.719	0.878
	ne2	0.728***				
Personality traits – openness (OP)	op1	0.681***	0.726	0.792	0.859	0.735
	op2	0.453***				
Digital anxiety (DA)	da_1	0.867***	0.561	0.819	0.574	0.693
	da_2	0.797***				
Online privacy concern (OPC)	opc_1	0.815***	0.778	0.871	0.786	0.692
	opc_2	0.814***				
	opc_3	0.866***				
Protective behavior (PB)	pb_1	0.797***	0.721	0.795	0.786	0.697
	pb_2	0.732***				
	pb_3	0.667***				
	pb_4	0.456***				
	pb_5	0.73***				
	pb_6	0.325***				

Notes: *** denotes significance level at $p < 0.01$. Abbreviations: CA - Cronbach's alpha, DG - Dillon-Goldstein's rho, CR - composite reliability, AVE - average variance extracted.

Source: Authors.

The discriminant validity of the measurement model represents the extent to which a construct is truly distinct from other constructs by empirical standards (Hair, Hult, Ringle, & Sarstedt, 2021), which can be examined through the Fornell-Larcker criterion. The Fornell-Larcker criterion, which compares the square root of AVE with correlations between latent variables, shows that the square root of AVE is larger than the largest correlation with any other construct in all cases (Table 7.3). Therefore, constructs considered in this study possess adequate discriminant validity.

Table 7.3. Fornell-Larcker criterion for assessing discriminant validity

	RES	SKILL	WEB	EX	AG	CO	NE	OP	DA	OPC	PB
RES	(0.689)										
SKILL	0.008	(0.824)									
WEB	0.057	0.248	(0.189)								
EX	0.001	0.002	0.001	(0.783)							
AG	0.011	0.001	0.003	0.134	(0.675)						
CO	0.003	0.001	0.011	0.024	0.036	(0.692)					
NE	0.014	0.002	0.008	0.014	0.008	0.001	(0.293)				
OP	0.007	0.002	0.003	0.005	0.011	0.013	0.001	(0.356)			
DA	0.034	0.001	0.001	0.01	0.016	0.001	0.001	0.001	(0.687)		
OPC	0.094	0.001	0.001	0.006	0.008	0.004	0.005	0.006	0.235	(0.682)	
PB	0.027	0.129	0.031	0.037	0.026	0.013	0.003	0.004	0.023	0.076	(0.427)

Notes: Square roots of average variance extracted (AVE), as discriminant value indicators, are shown on a diagonal line in parentheses. Abbreviations: RES - resilience to online privacy violation, SKILL - Internet skills, WEB - Internet activities, EX - personality traits - extraversion, AG - personality traits - agreeableness, CO - personality traits - conscientiousness, NE - personality traits - neuroticism, OP - personality traits - openness, DA - digital anxiety, OPC - online privacy concern, PB - protective behavior.

Source: Authors.

Model 1 was estimated using the ordinary least squares (OLS) method (Table 7.4). The model was estimated in two iterations so that more covariates were included in each successive iteration - version 1 is a simple case in which RES is regressed to other latent variables in the model and to two indicators of Internet use: Internet skills and variety of Internet use; and version 2, which includes all socio-demographic characteristics of the respondents.

Table 7.4. OLS estimation results of Model 1

Regressors	Version 1	Version 2
Internet skills	0.052	0.065
Internet range of activities	0.176**	0.132**
Time spent online	-0.015	-0.010
Online privacy concern	-0.231***	-0.218***
Digital anxiety	-0.073*	-0.085**
Social support	0.146***	0.133***
Protective behavior	0.101**	0.095**
Personality traits		
Extraversion	-0.080	-0.056
Agreeableness	0.089**	0.092**
Conscientiousness	0.048	0.047
Neuroticism	0.078**	0.077**
Openness	0.097***	0.098***
Socio-demographic characteristics		
Male		-0.072
Age		0.002
Household size		0.003
Education (benchmark: primary)		
Secondary		0.162
Tertiary		0.201
Post-graduate		0.080
Work status (benchmark: employed)		
Unemployed		0.309
Retired		0.095
Student		0.198
Settlement size (benchmark: less than 50,000)		
10,001–50,000		-0.040
50,001–100,000		-0.087
More than 100,000		-0.118
Household income (benchmark: less than 10,000 HRK)		
5,001–10,000 HRK		0.159
10,001–15,000 HRK		0.046
> 15,000 HRK		0.100
Region (benchmark: Pannonian Croatia)		
Adriatic Croatia		-0.018
City of Zagreb		-0.229
Northern Croatia		0.112
Number of observations	777	777
Adjusted R-squared	0.253	0.266

Notes: ***, **, and * denote significance level at $p < 0.01$, $p < 0.05$, and $p < 0.1$, respectively. Standard errors are omitted to conserve space. As of January 1, 2023, Croatia adopted the euro as its official currency with the official fixed exchange rate 1 EUR = 7.53450 HRK.

Source: Authors.

Before interpreting the results of the analysis, it should be pointed out that, given that the analysis is based on cross-sectional data (as opposed to a panel data structure), the analysis reveals only correlations or associations (instead of causation) and all the following results should be interpreted exclusively as such.

A unit standard deviation increase in estimated Internet range of activities was associated with a 0.176 to 0.132 standard deviation increase in resilience to OPVI. A unit standard deviation increase in estimated Internet skills was associated with a 0.052 to 0.065 standard deviation increase in online privacy concerns. However, neither this relationship, nor time spent online were found to be statistically significant in explaining variation in RES. Both social-psychological factors (digital anxiety and online privacy concern) proved to be statistically significant in both versions of Model 1. A unit standard deviation increase in digital anxiety was associated with a 0.073 to 0.085 standard deviation decrease in RES. Likewise, a unit standard deviation increase in an individual's online privacy concern was associated with a 0.231 to 0.218 standard deviation decrease in RES. Furthermore, social support and protective behavior were shown to exert a positive influence on individual resilience to OPVI. Finally, in terms of individual personality traits, agreeableness, neuroticism, and openness were shown to be associated with higher levels of resilience to OPVI.

In the second version of Model 1, of the eight analyzed socio-demographic factors, none of them were statistically significant in explaining variation in RES. This is somewhat surprising as one would expect younger, more educated people living in urban areas to be more resilient to OPVI as they likely have more experience in using the Internet. However, our results do not support this hypothesis, suggesting that resilience is not affected by any socio-demographic characteristic and is instead more associated with psychological factors.

Version 2 of Model 1 was also estimated using the ordered probit method (Table 7.5). The dependent variable in Model 1 RES can take on five different modalities (outcomes) measured on a Likert scale ranging from 1 to 5 (1 - Very low resilience, 2 - Low resilience, 3 - Neutral, 4 - High resilience, 5 - Very high resilience). These discrete outcomes were obtained by rounding

the RES value to the nearest whole number for each respondent and as such entered the ordered probit model. The other latent covariates still enter the equation in their standardized form and are therefore interpreted in standard deviation units.

Table 7.5. Ordered probit estimation results of Model 1

Regressors	Very low resilience	Low resilience	Neutral	High resilience	Very high resilience
Internet skills	-0.007	-0.014	-0.009	0.018	0.012
Internet range of activities	-0.012**	-0.025**	-0.015**	0.031**	0.022**
Time spent online	0.001	0.001	0.001	-0.001	-0.001
Online privacy concern	0.025***	0.050***	0.030***	-0.062***	-0.043***
Digital anxiety	0.006	0.013	0.008	-0.016	-0.011
Social support	-0.014***	-0.029***	-0.018***	0.036***	0.025***
Protective behavior	-0.010**	-0.021**	-0.013**	0.026**	0.018**
Personality traits					
Extraversion	0.006	0.013	0.008	-0.016	-0.011
Agreeableness	-0.008*	-0.015*	-0.009*	0.019*	0.013*
Conscientiousness	-0.007*	-0.014*	-0.009*	0.018*	0.012*
Neuroticism	-0.007*	-0.015*	-0.009*	0.018*	0.013*
Openness	-0.010***	-0.021***	-0.013***	0.026***	0.018***
Socio-demographic characteristics					
Male	0.008	0.016	0.010	-0.020	-0.014
Age	-0.000	-0.000	-0.000	0.000	0.000
Household size	0.001	0.002	0.001	-0.002	-0.001
Education (benchmark: primary)					
Secondary	-0.008	-0.015	-0.008	0.018	0.012
Tertiary	-0.009	-0.018	-0.010	0.022	0.015
Post-graduate	-0.004	-0.007	-0.003	0.008	0.005
Work status (benchmark: employed)					
Unemployed	-0.030	-0.069	-0.061	0.082	0.078
Retired	-0.006	-0.011	-0.006	0.013	0.009
Student	-0.020	-0.044	-0.032	0.054	0.042
Settlement size (benchmark: less than 50,000)					
10,001–50,000	0.006	0.013	0.008	-0.016	-0.011
50,001–100,000	0.001	0.002	0.001	-0.002	-0.002
More than 100,000	0.011	0.022	0.013	-0.027	-0.019
Household income (benchmark: less than 10,000 HRK)					
5,001–10,000 HRK	-0.019	-0.037	-0.021	0.046	0.031
10,001–15,000 HRK	-0.007	-0.013	-0.006	0.016	0.010
> 15,000 HRK	-0.013	-0.024	-0.012	0.030	0.019
Region (benchmark: Pannonian Croatia)					
Adriatic Croatia	0.004	0.008	0.005	-0.010	-0.007
City of Zagreb	0.032	0.056	0.023	-0.071	-0.041
Northern Croatia	-0.007	-0.017	-0.013	0.020	0.017
Number of observations	777	777	777	777	777

Notes: ***, **, and * denote significance level at $p < 0.01$, $p < 0.05$, and $p < 0.1$, respectively. Standard errors are omitted to conserve space. As of January 1, 2023, Croatia adopted the euro as its official currency with the official fixed exchange rate 1 EUR = 7.53450 HRK.

Source: Authors.

The results of the ordered probit model generally confirm the OLS results. A one standard deviation increase in range of Internet activities is associated with a 3.1 percent increase in the odds of an individual becoming highly resilient to OPVI and a 2.2 percent increase in the odds of being very highly resilient. This finding is consistent with the previous OLS result, which confirms that Internet users who perform a multitude of tasks on the Internet will be more resilient to OPVI. This model also shows no significant result regarding the Internet skills or the time spent online. Likewise, an increase of one standard deviation from the average online privacy concern translates into an increase in the probability of having very low resilience or low resilience (2.5 and 5.0 percent, respectively) and a decrease in the likelihood of being highly or very highly resilient to OPVI by 6.2 and 4.3 percent, respectively. This result is also consistent with previous OLS results indicating that people who are more concerned about their online privacy are less resilient to OPVI. Ordered probit results are also in line with OLS results in terms of protective behavior and social support, where a unit increase in these measures is associated with increased odds of being highly resilient or very highly resilient to OPVI. Regarding the individuals' personality traits, being more agreeable and open-minded is positively associated with the odds of being highly resilient or very highly resilient to OPVI. Finally, just like with OLS estimates, various socio-demographic characteristics are not statistically significant in explaining various outcomes in resilience to OPVI.

This study shows that Internet users with a higher level of digital literacy will be more resilient to online privacy violation incidents. However, the effect is greater on the side of increased range of Internet activities rather than on the side of Internet skills. The effect of the range of Internet activities as an antecedent to resilience to OPVI is fairly stable as more controls are added to the initial estimates (as we move from version 1 to version 2 of Model 1). This result can be explained by the fact that individuals who are more exposed to various activities performed on the Internet, regardless of their specific Internet skills, are simply more aware of all possible forms of violation of their privacy on the Internet, and therefore more resilient to any potential OPVI. As far as other variables are concerned, online privacy concern has the strongest negative effect on resilience to OPVI while social support has the

strongest positive effect. This result, combined with the observed importance of the variable approximating the variety of online activities used, leads to the conclusion that Internet users who are less concerned about their privacy, who perform various tasks on the Internet, and receive a high degree of social support from their close family, relatives, and friends, are more resilient to OPVI.

Anderson and Rainie (2014) point out that in the future privacy and control over personal information will become a luxury good and that only those with adequate digital literacy will be able to protect their privacy while for all others the perceived benefits of the Internet will outweigh the fear of OPVI. Further research explores how OPVI affects consumer behavior and changes in attitudes.

7.3. Consumers' attitude changes

In this chapter, we examine consumers' attitudes toward the Internet and consumer online behavior after an online privacy violation incident[16] in a more specific way. After a stressful event, do consumers use the Internet as much as before or do they change the way they use the Internet? Are they more cautious online? Do they change their attitudes toward the Internet accordingly? These issues are assessed by applying the concept of resilience and coping strategies in reaction to stress, whereas the focus of this empirical research is the change in online consumers' attitudes and behavior.

Studies on users' online attitudes emerged in the early days of the Internet (e.g., Schlosser, Shavitt, & Kanfer, 1999) and have gained importance as the online market developed (Cummins, Peltier, Schibrowsky, & Nill, 2014). Three main research streams support this study on how people deal with a stressful event and what consumers' responses to the OPVI are: consumer behavior in response to stress, coping strategies, and resilience.

16 Available as Škrinjarić, Budak, and Rajh (2022).

Subjective assessment of an incident as a privacy violation might vary from invasion of privacy and stalking behavior to violation of social norms (Moore, Moore, Shanahan, & Mack, 2015). OPVI in this research is regarded as a stressful event that might result in changes of consumer behavior online. In distinction to life-event stress, online privacy violation belongs to a consumption-induced source of stress that might result in consumption and non-consumption coping strategies or the combination of both. Non-consumption strategies, for example, involve ignoring the stressful event while deterring from certain online activity, using a compensatory strategy, looking for more information and seeking for warranties or completely ceasing the online activity (Moschis, 2007). According to Carver, Scheier, and Weintraub (1989), responses to an online privacy violation incident belong to the problem-focused coping that includes taking actions to remove the threat, planning future strategies, suppressing other activities to further focus on the solution, or restraint coping by holding back. Past research also recognizes situational coping with a specific event and emphasizes that individual differences in coping should be considered (Carver et al., 1989).

Coping is closely related to resilience. Resilience represents an individual's ability to recover from adversity, to overcome adversity, and/or to successfully adapt to it (McCubbin, 2001). Although definitions of resilience vary according to research field and context, a common understanding is that when exposed to threat or stress, individuals show a certain level of resilience enabling them to fully or partially recover, resist, adjust, and finally to stabilize their activity on the new level. The new equilibrium might be achieved by bouncing back, thriving, performing worse or better than before (as explained in detail in Chapter 4.5.6).

Translated into an individual consumer experience of online privacy violation, one could continue to use the Internet: (1) in the same manner as before (for the same online activities, as frequently as before, with the same level of caution, and with unchanged attitudes toward the Internet), (2) in a restricted way due to negative experience, or (3) more extensively compared to the online behavior prior to the incident. Changes in consumer attitudes may lead to consequently altering consumer behavior (Glasman & Albarracín, 2006), though not necessarily and not in the same direction. Although behavior might be restored after an OPVI,

attitudes might remain unrecovered and an inconsistency between behavior and attitudes might be observed (Maio et al., 2000).

We employed the survey data to test the following conceptual model:

$$ATT_i = \alpha + \beta_1 RES_i + \beta_2 PVC_i + \beta_3 SKILL_i + \beta_4 OAW_i + \beta_5 ST_i + \beta_6 GIAS_i + \beta_7 OPC_i + \beta_8 SH_i + \beta_9 TIME_i + y' X_i w + \varepsilon_i$$

where ATT is a general name for four different dependent variables representing consumers' attitudes toward the Internet after OPVI: (1) Internet usage after OPVI, (2) level of cautiousness on the Internet after OPVI, (3) range of activities performed on the Internet after OPVI, and (4) general attitude toward the Internet after OPVI. As for independent variables, RES is resilience to online privacy violation, privacy violation category (PVC) stands for type of OPVI, SKILL represents a measure of the consumer's Internet skills, OAW is online privacy awareness, ST is social trust, GIAS is general Internet attitude scale before OPVI, OPC is online privacy concern, SH is sharing private information online, TIME is number of hours spent online during the day, and X is a matrix of other socio-demographic characteristics of respondents used in the model.

A further point worth noting is that we measure the consumer's subjective assessment of OPVI, which does not necessarily mean that their privacy was violated in the true sense of privacy violation definition. For example, many respondents categorized "the use of cookies and personalized ads" as a violation of their online privacy. However, as all websites must comply with the ePrivacy Directive[17] , if a website complies with the so-called cookie law, the use of cookies and unwanted add-ons is not officially considered a breach of privacy. The privacy violation category (PVC) variable denotes OPVI type. Consumers with better computer skills (SKILL) are expected to be more active online and use the Internet for a wider range of operations. Richard, Chebat, Yang, and Putrevu (2010) found that more skilled Internet users have positive attitudes toward websites and show more exploratory behavior online. Online privacy awareness (OAW) is defined as individuals' consciousness regarding the importance

17 Available at https://gdpr.eu/cookies/

of online privacy and threats in an online environment, and it includes awareness of privacy policy practices in both public and private sectors (Malhotra et al., 2004). This relates to the individuals' desire for (sensitive) information control and to be familiarized about online privacy issues.

Online privacy concern (OPC) represents apprehension and uneasiness of an individual regarding the (mis)use of their sensitive personal data (Lwin et al., 2007), reflecting the degree of individuals' discomfort when online.

Online sharing of private information (SH) represents an individual's preferences about sharing private sensitive information online. The intensity of Internet usage, in terms of time spent online (TIME), could significantly determine different attitudes toward the Internet. Finally, consumer behavior and attitudes after the OPVI depend on socio-demographic characteristics of individual respondents (Martins, Yusuf, & Swanson, 2012; Cummins et al., 2014). Past research has reached no consensus about the significance and direction of the relationship, so it would be interesting to shed more light on the individual socio-demographics and online privacy concern nexus. Therefore, demographic characteristics of the Internet users were included in the model in terms of gender, age, level of education, occupation, and household size. Furthermore, we wanted to examine if there were any regional differences across five regions in Croatia and among respondents living in larger (urban) or smaller (rural) places of residence. The difference in the place of residence size is a proxy for capturing differences between the urban and the rural environment in Croatia. People living in rural environments might be less concerned about privacy when online because they openly interact more with each other, and privacy is harder to keep in everyday life in smaller places.

Our empirical methodology consists of two parts. In the first step, we test the reliability, consistency, and dimensionality of latent constructs used in our model. The reliability and consistency were analyzed by Cronbach's alpha (CA) coefficient, alpha-if-deleted indicator, and different correlations, while the dimensionality was examined by exploratory factor analysis. In the second step, once the latent constructs (variables) were estimated and

tested, the research model was estimated using OLS and ordered probit techniques.

Each column represents a separate model with four different dependent variables (Table 7.6). Prior to the analysis of the results, we would like to point out that, as we are dealing with a cross-section type of dataset (as opposed to panel structure), our analysis only reveals correlations or associations (rather than causation), and all the following results should be interpreted as such.

Table 7.6. OLS estimation results

	Internet usage after OPVI (1)	Cautiousness on the Internet after OPVI (2)	Range of activities on the Internet after OPVI (3)	Attitude toward the Internet after OPVI (4)
Resilience to OPVI	0.206***	-0.213***	0.159***	0.218***
	(0.034)	(0.032)	(0.035)	(0.032)
Online privacy awareness	-0.039	0.107***	-0.060*	-0.018
	(0.033)	(0.031)	(0.033)	(0.031)
Social trust	-0.002	-0.095***	0.017	0.123***
	(0.031)	(0.029)	(0.031)	(0.029)
General Internet attitude	0.111***	0.037	0.112***	0.210***
	(0.033)	(0.030)	(0.033)	(0.031)
Online privacy concern	-0.030	0.231***	-0.083**	-0.131***
	(0.034)	(0.032)	(0.034)	(0.032)
Sharing private information online	0.080**	-0.112***	0.078**	0.066**
	(0.035)	(0.033)	(0.035)	(0.033)
Internet skills	0.102***	0.044	0.084**	0.019
	(0.037)	(0.034)	(0.037)	(0.035)
Hours spent online	0.041***	0.004	0.028***	0.016
	(0.010)	(0.010)	(0.011)	(0.010)
Male	0.024	0.049	0.112*	0.032
	(0.063)	(0.058)	(0.063)	(0.059)
Household size	0.037*	-0.018	0.025	0.046**
	(0.022)	(0.021)	(0.022)	(0.021)
Online privacy violation category (benchmark: unwanted commercials)				
Intrusion into e-mail or SN account	0.026	0.398***	-0.167*	0.025
	(0.100)	(0.093)	(0.101)	(0.094)
Recording locations, conversations, searches, messages	-0.059	0.003	-0.004	-0.210***
	(0.077)	(0.071)	(0.078)	(0.072)
Scam	0.247	0.278	0.168	-0.039
	(0.188)	(0.174)	(0.189)	(0.177)
Personal information theft w/o financial costs	-0.178	0.357***	-0.128	-0.207*
	(0.127)	(0.117)	(0.128)	(0.119)
Personal information theft with financial costs	-0.365**	0.741***	-0.205	-0.110
	(0.172)	(0.159)	(0.173)	(0.161)
Other	-0.311**	0.260*	-0.299*	-0.231
	(0.157)	(0.145)	(0.158)	(0.147)

	Internet usage after OPVI (1)	Cautiousness on the Internet after OPVI (2)	Range of activities on the Internet after OPVI (3)	Attitude toward the Internet after OPVI (4)
Age (benchmark: 18–34)				
35–50	0.120	-0.022	0.006	0.200**
	(0.084)	(0.077)	(0.084)	(0.079)
50+	0.109	-0.097	0.219**	0.194**
	(0.099)	(0.092)	(0.100)	(0.093)
Education (benchmark: secondary education or less)				
Higher education	-0.060	-0.081	-0.158**	-0.055
	(0.078)	(0.072)	(0.079)	(0.074)
Occupation (benchmark: self-employed)				
Manager	0.186	-0.064	-0.072	-0.084
	(0.198)	(0.183)	(0.199)	(0.186)
Professional	0.308*	0.081	0.162	-0.166
	(0.163)	(0.151)	(0.164)	(0.153)
Technician/clerk	0.229	0.015	-0.095	-0.122
	(0.155)	(0.143)	(0.156)	(0.146)
Worker	0.360**	0.037	-0.122	-0.136
	(0.154)	(0.142)	(0.155)	(0.145)
Retired	0.407**	-0.038	0.002	0.016
	(0.163)	(0.151)	(0.164)	(0.153)
Student	0.144	0.033	-0.092	-0.028
	(0.177)	(0.164)	(0.178)	(0.166)
Unemployed	0.453***	-0.084	0.013	0.108
	(0.169)	(0.156)	(0.170)	(0.159)
City size (benchmark: 10,000 or less)				
10,000–50,000	-0.021	-0.119	0.130	-0.044
	(0.080)	(0.074)	(0.080)	(0.075)
50,001–100,000	-0.100	-0.018	-0.001	-0.048
	(0.128)	(0.118)	(0.129)	(0.120)
More than 100,000	-0.031	-0.147*	0.045	0.067
	(0.089)	(0.082)	(0.089)	(0.083)
NUTS2 region (benchmark: Pannonian Croatia)				
Adriatic Croatia	0.131	0.027	-0.000	0.074
	(0.082)	(0.076)	(0.082)	(0.077)
City of Zagreb	0.229**	0.122	0.178	0.369***
	(0.114)	(0.106)	(0.115)	(0.107)
Northern Croatia	0.249***	-0.040	0.107	0.223***
	(0.092)	(0.085)	(0.092)	(0.086)
N	1,000	1,000	1,000	1,000
R-squared	0.153	0.278	0.142	0.254
Adjusted R-squared	0.125	0.255	0.114	0.229

Notes: Standard errors in parentheses; ***, **, and * denote significance level at $p < 0.01$, $p < 0.05$, and $p < 0.10$, respectively. Benchmark levels of certain socio-demographic variables were chosen based on our intuition.

Source: Authors.

Resilience to OPVI is significantly associated with all four dependent variables, with the strongest effect for attitude toward the Internet after an OPVI - on average, an increase of one standard deviation in resilience, ceteris paribus, is associated with an increase of 0.218 standard deviations in attitude toward the Internet after OPVI. A similar interpretation stands for Internet usage after OPVI and the range of activities on the Internet after OPVI. The direction of association is reversed for level of cautiousness on the Internet after OPVI - on average, an increase of one standard deviation in resilience, ceteris paribus, is associated with a decrease of 0.213 standard deviations in cautiousness on the Internet after OPVI.

Regarding other latent regressors, focusing only on statistically significant results, online privacy awareness is positively associated with cautiousness and negatively with the range of activities; social trust is negatively correlated with cautiousness and positively with general attitude; general Internet attitude before OPVI is positively associated with the Internet usage, range of activities, and general Internet attitude after OPVI; online privacy concern is positively correlated with the level of cautiousness and negatively with the range of activities and attitude toward the Internet; and sharing private information online is positively associated with the Internet usage, the range of activities, and attitude toward the Internet and negatively associated with the level of cautiousness. Both Internet skills and hours spent online are positively associated with the Internet usage and the range of activities after OPVI.

Regarding OPVI categories, compared to someone who experienced unwanted commercials (somewhat harmless form of OPVI), the greatest effects are for people who experienced personal information theft with financial costs - they recorded reduced Internet usage after OPVI and increased levels of cautiousness on the Internet after OPVI. Additionally, people who experienced intrusion into e-mail or social network accounts and personal information theft without financial costs also recorded higher levels of cautiousness on the Internet after OPVI.

Finally, regarding demographic factors, gender, age, household size, education level, occupation, and settlement size showed to be of no statistical significance, or only weak

statistical significance, in explaining variation in any of the four dependent variables. There are, however, two exceptions to this: firstly, compared to people who are self-employed, workers, retirees, and the unemployed showed greater Internet usage even after OPVI; and secondly, compared to young adults aged 18-34, people in age groups 35-50 and 50+ had more positive attitudes toward the Internet after OPVI. Lastly, compared to someone living in Pannonian Croatia, people located in the City of Zagreb (capital of Croatia) and Northern Croatia use the Internet more and have a more positive general attitude toward the Internet even after an OPVI.

Model 1 was also estimated, using the ordered probit technique, to estimate the probability of each outcome of each dependent variable. In this case, dependent variables enter the model as discrete variables with their outcomes ranging from 1 to 5, while latent covariates still enter the equation in their standardized form and are hence interpreted in terms of standard deviations. The results of ordered probit estimations (Table 7.7) are presented in four different panels, each for every different dependent variable, whose discrete outcomes are listed in the first row of each panel.

Table 7.7. Ordered probit estimation results

Panel A: Internet usage after OPVI

	Much less frequently (1)	Less frequently (2)	The same (3)	More frequently (4)	Much more frequently (5)
Resilience to OPVI	-0.004***	-0.050***	0.043***	0.008***	0.003**
	(0.001)	(0.009)	(0.008)	(0.002)	(0.001)
Online privacy awareness	0.001	0.009	-0.008	-0.001	-0.001
	(0.001)	(0.008)	(0.007)	(0.001)	(0.001)
Social trust	-0.000	-0.001	0.001	0.000	0.000
	(0.001)	(0.007)	(0.006)	(0.001)	(0.001)
General Internet attitude	-0.002**	-0.023***	0.020***	0.004**	0.002**
	(0.001)	(0.007)	(0.007)	(0.001)	(0.001)
Online privacy concern	0.001	0.009	-0.007	-0.001	-0.001
	(0.001)	(0.008)	(0.007)	(0.001)	(0.001)
Sharing private information online	-0.001*	-0.020**	0.017**	0.003**	0.001*
	(0.001)	(0.009)	(0.007)	(0.001)	(0.001)

Panel B: Level of cautiousness on the Internet after OPVI

	Dramatically decreased (1)	Slightly decreased (2)	Remained the same (3)	Slightly increased (4)	Dramatically increased (5)
Resilience to OPVI	0.001	0.008***	0.097***	-0.042***	-0.063***
	(0.001)	(0.002)	(0.015)	(0.008)	(0.010)
Online privacy awareness	-0.000	-0.004***	-0.051***	0.022***	0.033***
	(0.000)	(0.001)	(0.014)	(0.007)	(0.009)
Social trust	0.000	0.003***	0.045***	-0.020***	-0.029***
	(0.000)	(0.001)	(0.013)	(0.006)	(0.009)
General Internet attitude	-0.000	-0.001	-0.017	0.007	0.011
	(0.000)	(0.001)	(0.014)	(0.006)	(0.009)
Online privacy concern	-0.001	-0.008***	-0.107***	0.047***	0.069***
	(0.001)	(0.002)	(0.015)	(0.008)	(0.010)
Sharing private information online	0.000	0.004***	0.053***	-0.023***	-0.035***
	(0.000)	(0.001)	(0.015)	(0.007)	(0.010)

Panel C: Range of activities performed on the Internet after OPVI

	Dramatically decreased (1)	Slightly decreased (2)	Remained the same (3)	Slightly increased (4)	Dramatically increased (5)
Resilience to OPVI	-0.007***	-0.044***	0.035***	0.014***	0.001*
	(0.002)	(0.010)	(0.009)	(0.004)	(0.001)
Online privacy awareness	0.003*	0.018*	-0.015*	-0.006*	-0.001
	(0.002)	(0.009)	(0.008)	(0.003)	(0.000)
Social trust	-0.000	-0.002	0.001	0.000	0.000
	(0.001)	(0.009)	(0.007)	(0.003)	(0.000)
General Internet attitude	-0.004***	-0.029***	0.024***	0.009***	0.001*
	(0.002)	(0.009)	(0.008)	(0.003)	(0.001)
Online privacy concern	0.004**	0.025**	-0.020**	-0.008**	-0.001
	(0.002)	(0.010)	(0.008)	(0.003)	(0.000)
Sharing private information online	-0.003**	-0.022**	0.018**	0.007**	0.001
	(0.002)	(0.010)	(0.008)	(0.003)	(0.000)

Panel D: Attitude toward the Internet after OPVI

	Much more negative (1)	More negative (2)	Unchanged (3)	More positive (4)	Much more positive (5)
Resilience to OPVI	-0.016***	-0.093***	0.102***	0.005***	0.002**
	(0.003)	(0.015)	(0.016)	(0.002)	(0.001)
Online privacy awareness	0.001	0.003	-0.004	-0.000	-0.000
	(0.002)	(0.013)	(0.014)	(0.001)	(0.000)
Social trust	-0.009***	-0.055***	0.060***	0.003***	0.001**
	(0.003)	(0.013)	(0.014)	(0.001)	(0.001)
General Internet attitude	-0.014***	-0.084***	0.092***	0.005***	0.002**
	(0.003)	(0.014)	(0.015)	(0.001)	(0.001)
Online privacy concern	0.010***	0.061***	-0.067***	-0.003***	-0.001**
	(0.003)	(0.014)	(0.015)	(0.001)	(0.001)
Sharing private information online	-0.005*	-0.029**	0.031**	0.002*	0.001
	(0.003)	(0.014)	(0.016)	(0.001)	(0.000)

Notes: Standard errors in parentheses; ***, **, and * denote significance level at $p < 0.01$, $p < 0.05$, and $p < 0.10$, respectively.

Source: Authors.

Focusing on the first dependent variable - Internet usage after OPVI - ordered probit results show that an increase of one standard deviation in resilience to OPVI is associated with a 5.0 percent decrease in probability to use the Internet less frequently, and with a 4.3 percent increase in probability to use the Internet the same as before OPVI. This finding is in line with the previous OLS result confirming that Internet users with higher resilience to OPVI are more likely to use the Internet the same or more frequently after an OPVI occurred. A similar interpretation stands for general Internet attitude and sharing private information online variables.

Regarding the second dependent variable - level of cautiousness on the Internet after OPVI - results show that an increase of one standard deviation in resilience to OPVI is associated with a 9.7 percent increase in probability to be as cautious while browsing the Internet as before an OPVI; and also, with a 4.2 percent and 6.3 percent decrease in the probability of slightly increasing or dramatically increasing the level of cautiousness, respectively. This finding is also in line with the previous OLS result confirming that Internet users with higher resilience to OPVI are more likely not to change their level of cautiousness while online. Online privacy awareness and online privacy concern both have similar results - an increase in one standard deviation unit in these variables is associated with a 5.1 percent and 10.7 percent decrease in probability, respectively, to remain equally cautious on the Internet after an OPVI; a 2.2 percent and 4.7 percent increase in the probability of slightly increasing the level of cautiousness; and a 3.3 percent and 6.9 percent increase in the probability of dramatically increasing the level of cautiousness. Thus, people with higher online privacy awareness and online privacy concern are more likely to increase their cautiousness on the Internet after an OPVI. Like these two regressors, social trust and sharing private information online also have very similar results - an increase in one standard deviation unit in these variables is associated with a 4.5 percent and 5.3 percent increase in probability, respectively, to remain equally cautious on the Internet after an OPVI; a 2.0 percent and 2.3 percent decrease in the probability of slightly increasing the level of cautiousness; and a 2.9 percent and 3.5 percent decrease in the probability of dramatically increasing the level of cautiousness.

Regarding the range of activities performed on the Internet after an OPVI, more resilient individuals are less likely (-4.4 percent) to slightly decrease their range of Internet activities and are more likely to either have the same range of activities (3.5 percent) or even increase their range of activities (1.4 percent). Interestingly, individuals with a more favorable general Internet attitude are most likely to decrease their range of activities after an OPVI (-2.9 percent) or to keep the same range of activities (2.4 percent).

Finally, regarding the attitude of the respondents toward the Internet after an OPVI, individuals who are more resilient, with greater level of social trust, and with better general Internet attitude, are most likely not to change their attitude toward the Internet (10.2 percent, 6.0 percent, and 9.2 percent, respectively), and are less likely to have a more negative attitude (-9.3 percent, -5.5 percent, and -8.4 percent, respectively).

This research analyzes consumers' attitudes in the context of their reaction to a stressful event, specifically to an experience of online privacy violation. The results show that resilience of consumers helps them maintain similar attitudes and online behavior after a privacy violation incident. Companies and regulators should work on reducing privacy concerns and perceived risks of online users to prevent changing positive attitudes toward the use of the Internet into negative ones.

Preliminary analysis[18] showed that resilience to OPVI affects people's attitudes and behavior as citizens regarding the use of digital public services. On the one hand, we are witnessing the growing digitalization of public services, accompanied by increased privacy risk, and on the other, there is a rising necessity to "go digital" (e.g., in smart cities or in times of a pandemic). The individuals' opinions on the usage of digital public services (DPS) in general and local digital public services (LDPS) at the city or municipality level are captured by four respective items in the questionnaire (Appendix 2 and Appendix 3). They measure the intention to use online public services after experiencing an OPVI. The analysis showed that more resilient Internet users (citizens), even though they had been victims of an online privacy breach, tend to use digital public services more than their less resilient fellow citizens.

18 The paper on this part of the research is under review for publication in a journal so it was not possible to publish the full research in this book.

8. Conclusion

The ultimate objective of the REPRICON research was to empirically test the model of individual resilience to online privacy violation. Therefore, after empirically assessing selected relations among the variables, we have included all variables in the model and tested the total of 21 hypotheses using the SEM-PLS technique[19]. In the center of the model is resilience of an individual Internet user (consumer, citizen) in Croatia who had subjectively gone through some kind of privacy infringement online.

Internet users in Croatia have developed a certain level of resilience to online privacy breaches (> 3 on a scale of 1 to 5). For most respondents, it did not take too much time and trouble to recover from the most recent OPVI they experienced.

The rather fast and easy recovery associated with the observed resilience to OPVI was expected given that most of the reported cases of OPVI were self-categorized by respondents as less severe. Annoying advertisements, unwanted commercials, and recording the user's location and activities when online are the most reported OPVIs, hence without financial losses.

The results show that variation in individual resilience to online privacy violation is explained primarily by personality traits. Regardless of gender, age, income, education attained, or regional (urban vs. rural) residence, a more open and extroverted person would more easily cope with the stress an online privacy incident would cause. In contrast, neuroticism as a personality trait would make Internet users less resilient to OPVI. Psychological factors do explain behavior in online settings and should be included in online user behavior studies.

Despite being concerned for their online privacy, Internet users on average are willing to trade off some privacy for the benefits offered by using the Internet. Further, those who see positive outcomes of using the Internet would recover faster or cope easier with the OPVI.

19 The paper on this part of the research is under review for publication in a journal so it was not possible to publish the full research in this book.

The highest concern about online privacy is reported about extensive collection of personal information over the Internet. Online privacy concern weakens individual resilience to OPVI, as does digital anxiety: Internet users who feel worried about the digitalization process and express aversion toward computers and advanced ICT, demonstrate less resilience to OPVI. Similarly, Internet users with better digital skills and advanced Internet literacy are more resilient to OPVI. Further, a wide range of activities an Internet user performs online, including more complex ones, is associated with more resilience, regardless of the time a person spends on the Internet.

Victims of online privacy breaches take some preventive measures employing privacy protective behavior actions. Since their online privacy awareness is rather low, and given they are not so familiar with privacy issues and available solutions that companies and the government employ to protect their privacy, most Internet users affected by OPVI choose not to provide personal information to untrustworthy websites and only fill out data partially when registering to certain websites.

The main finding of the REPRICON project is that, after being victims of online privacy violation, more resilient Internet users would continue to perform their activities online at the same or even higher level than before the incident. The “bounce back” will be faster and more intense if the online privacy breach is perceived less serious. Thus, we have confirmed that behavioral outcomes after online privacy violation depend on individual resilience. Given that Internet users are individuals acting as consumers and citizens, our results have diverse policy implications.

Companies should acknowledge that their customers understand unwanted commercials and advertisements as an attack on their privacy and should react accordingly. Even legally recognized “cookies”, recording location or tracing past online activity to improve service offered to the user would cause distress to some clients since they would consider this to be a privacy infringement. Websites should be clear about their data-gathering policies and how this information is used to mitigate online privacy concern and build resilience to subjectively

perceived online privacy violation incidents. Although even moderately resilient consumers do not refrain from e-buying, more resilient consumers would easily continue their activities online and supposedly would not be reluctant to accept new online products and services. One should not expect resilience to OPVI to grow naturally with the future prevalence of consumers belonging to younger, digital native generations. Consumers with better digital skills would know how to employ advanced techniques to protect their privacy online, at least to the extent they estimate as necessary. The upcoming generations have rather low resilience to OPVI and therefore the balance between the perceived risk and benefits of using the Internet could be established at a lower level than marketers would hope for. Both businesses and governments should improve the way privacy protection policy is implemented.

Privacy protection and clear communication are crucial for the success of the digitalization process. Given the low trust in government privacy protection policies and the low trust in institutions in general, any subjective notion of privacy infringement might deter citizens from wider usage of digital public services.

9. Closing remarks

Almost four years have passed since we started to work on the REPRICON project and although there is still much to do in the last five months of the project, this book must be completed. Some papers are still pending for publication in journals, so the book does not contain all our work in detail. The book should be produced for the final REPRICON conference planned in November 2023 as this is an excellent occasion to show it to our colleagues and the wider public. The book will be available online at the Institute's website, as well as information about upcoming publications and future research endeavors.

Your REPRICON team

References

1. Ab Hamid, N. R. (2008). Consumers' behaviour towards internet technology and internet marketing tools. International Journal of Communications, 2(3), 195–204.
2. Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. Science, 347(6221), 509–514. doi: https://doi.org/10.1126/science.aaa1465
3. Adger, W. N. (2000). Social and ecological resilience: Are they related? Progress in Human Geography, 24(3), 347–364. doi: https://doi.org/10.1191/030913200701540465
4. Adger, W. N. (2003). Building resilience to promote sustainability. IHDP Update, 2, 1–3.
5. Adger, W. N., Hughes, T. P., Folke, C., Carpenter, S. R., & Rockström, J. (2005). Social-ecological resilience to coastal disasters. Science, 309, 1036–1039. doi: https://doi.org/10.1126/science.1112122
6. Afolabi, O. O., Ozturen, A., & Ilkan, M. (2021). Effects of privacy concern, risk, and information control in a smart tourism destination. Economic Research-Ekonomska Istraživanja, 34(1), 3119–3138. doi: https://doi.org/10.1080/1331677X.2020.1867215
7. Agaibi, C. E., & Wilson, J. P. (2005). Trauma, PTSD, and resilience: A review of the literature. Trauma, Violence, & Abuse, 6(3), 195-216. doi: https://doi.org/10.1177/1524838005277438
8. Ahmad, S., Feder, A., Lee, E. J., Wang, Y., Southwick, S. M., Schlackman, E., … Charney, D. S. (2010). Earthquake impact in a remote South Asian population: Psychosocial factors and posttraumatic symptoms. Journal of Traumatic Stress, 23(3), 408–412. doi: https://doi.org/10.1002/jts.20535
9. Ahmed, R., Seedat, M., van Niekerk, A., & Bulbulia, S. (2004). Discerning community resilience in disadvantaged communities in the context of violence and injury prevention. South African Journal of Psychology, 34, 386–408. doi: https://doi.org/10.1177/008124630403400304
10. Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179–211. doi: https://doi.org/10.1016/0749-5978(91)90020-T
11. Akman, I., & Rehan, M. (2014). Online purchase behaviour among professionals: A socio-demographic perspective for Turkey. Economic Research-Ekonomska Istraživanja, 27(1), 689–699. doi: https://doi.org/10.1080/1331677X.2014.975921

12. Al Nuaimi, E., Al Neyadi, H., Mohamed, N., & Al-Jaroodi, J. (2015). Applications of big data to smart cities. Journal of Internet Services and Applications, 6(1), 1-15. doi: https://doi.org/10.1186/s13174-015-0041-5

13. Allen, J. (2015). Online privacy and hacking. San Diego, CA: Reference Point Press.

14. Allenby, B., & Fink, J. (2005). Toward inherently secure and resilient societies. Science, 309(5737), 1034–1036. doi: https://doi.org/10.1126/science.1111534

15. Altay, N., & Green, W. G., III. (2006). OR/MS research in disaster operations management. European Journal of Operational Research, 17, 475–493. doi: https://doi.org/10.1016/j.ejor.2005.05.016

16. Amro, B. (2018). Phishing techniques in mobile devices. Journal of Computer and Communications, 6(2), 27–35. doi: https://doi.org/10.4236/jcc.2018.62003

17. Anderson, J., & Rainie, L. (2014). Digital life in 2015. Washington, DC: Pew Research Center.

18. Androniceanu, A., Kinnunen, J., Georgescu, I., & Androniceanu, A. M. (2020). Multidimensional analysis of consumer behavior on the European digital market. In W. Stroka (Ed.), Perspectives on consumer behaviour: Theoretical aspects and practical applications (pp. 75–95). Cham: Springer. doi: https://doi.org/10.1007/978-3-030-47380-8_4

19. Anić, I.-D., Budak, J., Rajh, E., Recher, V., Škare, V., & Škrinjarić, B. (2018). Extended model of online privacy concern: What drives consumers' decisions? Online Information Review, 43(5), 799–817. doi: https://doi.org/10.1108/OIR-10-2017-0281

20. Anić, I.-D., Škare, V., & Kursan Milaković, I. (2019). The determinants and effects of online privacy concerns in the context of e-commerce. Electronic Commerce Research and Applications, 36, 100868. doi: https://doi.org/10.1016/j.elerap.2019.100868

21. Annalakshmi, N. (2007). Resilience in relation to extraversion-introversion, psychoticism, and neuroticism. Indian Journal of Psychometry and Education, 38, 51–55.

22. Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. Computer Networks, 54(15), 2787–2805. doi: https://doi.org/10.1016/j.comnet.2010.05.010

23. Avey, J. B., Reichard, R. J., Luthans, F., & Mhatre, K. H. (2011). Meta-analysis of the impact of positive psychological capital on employee attitudes, behaviors, and performance. Human Resource Development Quarterly, 22(2), 127–152. doi: https://doi.org/10.1002/

hrdq.20070

24. Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. MIS Quarterly, 30(1), 13–28. doi: https://doi.org/10.2307/25148715

25. Bădîrcea, R. M., Manta, A. G., Florea, N. M., Popescu, J., Manta, F. L., & Puiu, S. (2021). E-commerce and the factors affecting its development in the age of digital technology: Empirical evidence at EU-27 level. Sustainability, 14(1), 101. doi: https://doi.org/10.3390/su14010101

26. Baek, Y. M., Kim, E.-M., & Bae, Y. (2014). My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns. Computers in Human Behavior, 31, 48–56. doi: https://doi.org/10.1016/j.chb.2013.10.010

27. Bakker, A. B., Van Der Zee, K. I., Lewig, K. A., & Dollard, M. F. (2006). The relationship between the big five personality factors and burnout: A study among volunteer counselors. The Journal of Social Psychology, 146(1), 31–50. doi: https://doi.org/10.3200/SOCP.146.1.31-50

28. Bansal, G., & Zahedi, F. M. (2015). Trust violation and repair: The information privacy perspective, Decision Support Systems, 71, 62–77. doi: https://doi.org/10.1016/j.dss.2015.01.009

29. Bansal, G., Zahedi, F. M., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. Decision Support Systems, 49(2), 138–150. doi: https://doi.org/10.1016/j.dss.2010.01.010

30. Bartoli, A., Hernández-Serrano, J., Soriano, M., Dohler, M., Kountouris, A., & Barthel, D. (2011). Security and privacy in your smart city. Proceedings of the Barcelona Smart Cities Congress, 292, 1–6. Retrieved from: https://docplayer.net/3235974-Security-and-privacy-in-your-smart-city.html

31. Bartone, T. (1989). Predictors of stress-related illness in city bus drivers. Journal of Occupational Medicine, 31(8), 657–663. doi: https://doi.org/10.1097/00043764-198908000-00008

32. Basin, D., Cremers, C., Kim, T. H. J., Perrig, A., Sasse, R., & Szalachowski, P. (2016). Design, analysis, and implementation of ARPKI: An attack-resilient public-key infrastructure.

IEEE Transactions on Dependable and Secure Computing, 15(3), 393–408. doi: https://doi.org/10.1109/TDSC.2016.2601610

33. Baumeister, R. F., & Leary, M.R. (1997). Writing narrative literature reviews. Review of General Psychology, 1(3), 311–320. doi: https://doi.org/10.1037/1089-2680.1.3.311

34. Beckers, K., & Pape, S. (2016, September). A serious game for eliciting social engineering security requirements. 2016 IEEE 24th International Requirements Engineering Conference (RE), 16–25. doi: https://doi.org/10.1109/re.2016.39

35. Beke, F. T., Eggers, F., & Verhoef, C. (2018). Consumer informational privacy: Current knowledge and research directions. Foundations and Trends in Marketing, 11(1), 1–71. doi: https://doi.org/10.1561/1700000057

36. Bélanger, F., Hiller, J., & Smith, W. (2002). Trustworthiness in electronic commerce: The role of privacy, security and site attributes. Journal of Strategic Information Systems, 11(3–4), 245–270. doi: https://doi.org/10.1016/S0963-8687(02)00018-5

37. Beltman, S., Mansfield, C., & Price, A. (2011). Thriving not just surviving: A review of research on teacher resilience. Educational Research Review, 6(3), 185–207. doi: https://doi.org/10.1016/j.edurev.2011.09.001

38. Bergeman, C. S., Chlpuer, H. M., Plomin, R., Pedersen, N. L., McClearn, G. E., Nesselroade, J. R., Costa, P. T., Jr., & McCrae, R. R. (1993). Genetic and environmental effects on openness to experience, agreeableness, and conscientiousness: An adoption/twin study. Journal of Personality, 61(2), 159–179. doi: https://doi.org/10.1111/j.1467-6494.1993.tb01030.x

39. Bhamra, R., Dani, S., & Burnard, K. (2011). Resilience: The concept, a literature review and future directions. International Journal of Production Research, 49(18), 5375–5393. doi: https://doi.org/10.1080/00207543.2011.563826

40. Bhattacharyya, A., & Belk, R. W. (2019). Consumer resilience and subservience in technology consumption by the poor. Consumption Markets & Culture, 22(5–6), 489–507. doi: https://doi.org/10.1080/10253866.2018.1562686

41. Bidgoli, H. (2006). Handbook of information security: Key concepts, infrastructure, standards, and protocols (Vol. 1). John Wiley & Sons, Inc.

42. Blakley, B., McDermott, E., & Geer, D. (2001, September). Information security

is information risk management. Proceedings of the 2001 Workshop on New Security Paradigms, 97–104. doi: https://doi.org/10.1145/508171.508187

43. Block, J. (2002). Personality as an affect-processing system. Mahwah, NJ: Erlbaum. doi: https://doi.org/10.4324/9781410602466

44. Block, J. H., & Block, J. (1980). The role of ego-control and ego-resilience in the organization of behavior. In W. A. Collins (Ed.), Development of cognition, affect and social relations: The Minnesota symposia on child psychology (Vol. 13, pp. 39–101). Hillsdale, NJ: Erlbaum.

45. Block, J., & Turula, E. (1963). Identification, ego control, and adjustment. Child Development, 34(4), 945–953. doi: https://doi.org/10.2307/1126537

46. Bodin, P., & Wiman, B. (2004). Resilience and other stability concepts in ecology: Notes on their origin, validity, and usefulness. ESS Bulletin, 2(2), 33–43.

47. Bogar, C. B., & Hulse-Killacky, D. (2006). Resiliency determinants and resiliency processes among female adult survivors of childhood sexual abuse. Journal of Counseling & Development, 84(3), 318–327. doi: https://doi.org/10.1002/j.1556-6678.2006.tb00411.x

48. Bolger, N. (1990). Coping as a personality process: A prospective study. Journal of Personality and Social Psychology, 59, 525–537. doi: https://doi.org/10.1037/0022-3514.59.3.525

49. Bonanno, G. A. (2004). Loss, trauma, and human resilience: Have we underestimated the human capacity to thrive after extremely aversive events? The American Psychologist, 59(1), 20–28. doi: https://doi.org/10.1037/0003-066X.59.1.20

50. Bonanno, G. A., Galea, S., Bucciarelli, A., & Vlahov, D. (2007). What predicts psychological resilience after disaster? The role of demographics, resources and life stress. Journal of Consulting and Clinical Psychology, 75(5), 671–682. doi: https://doi.org/10.1037/0022-006X.75.5.671

51. Bonanno, G. A., Romero, S. A., & Klein, S. I. (2015). The temporal elements of psychological resilience: An integrative framework for the study of individuals, families, and communities. Psychological Inquiry, 26, 139–169. doi: http://dx.doi.org/10.1080/1047840X.2015.992677

52. Bourbeau, P. (2013). Resiliencism: Premises and promises in securitisation research.

Resilience, 1(1), 3–17. doi: https://doi.org/10.1080/21693293.2013.765738

53. Bradshaw, S. D. (1997). Impression management and the NEO five-factor inventory: Cause for concern? Psychological Reports, 80(3), 832–834. doi: https://doi.org/10.2466/pr0.1997.80.3.832

54. Brand, F. S., & Jax, K. (2007). Focusing the meaning(s) of resilience: Resilience as a descriptive concept and a boundary object. Ecology and Society, 12(1), 23. doi: https://doi.org/10.5751/ES-02029-120123

55. Brown, B. B., & Perkins, D. D. (1992). Disruptions in place attachment. In Place attachment (pp. 279-304). Boston, MA: Springer US. doi: https://doi.org/10.1007/978-1-4684-8753-4_13

56. Brissette, I., Scheier, M. F., & Carver, C. S. (2002). The role of optimism in social network development, coping, and psychological adjustment during a life transition. Journal of Personality and Social Psychology, 82(1), 102–111. doi: https://doi.org/10.1037//0022-3514.82.1.102

57. Bruneau, M., Chang, S. E., Eguchi, R. T., Lee, G. C., O'Rourke, T. D., Reinhorn, A. M. … von Winterfeldt, D. (2003). A framework to quantitatively assess and enhance the seismic resilience of communities. Earthquake Spectra, 19(4), 733–752.

58. Buchanan, T., Paine, C., Joinson, A. N., & Reips, U.-D. (2007). Development of measures of online privacy concern and protection for use on the internet. Journal of the American Society for Information Science and Technology, 58(2), 157–165. doi: https://doi.org/10.1002/asi.20459

59. Budak, J., & Rajh, E. (2022). Consumer online behavior in the European digital agenda context: Should we rely on a privacy paradox? 9th REDETE Conference on Researching Economic Development and Entrepreneurship in Transition Economies: Proceedings, 332–341. Banja Luka: Faculty of Economics, University of Banja Luka.

60. Budak, J., Rajh, E., Slijepčević, S., & Škrinjarić, B. (2020). Theoretical concepts of consumer resilience to online privacy violation. EIZ Working Paper No. 2003. Retrieved from: https://hrcak.srce.hr/245205

61. Budak, J., Rajh, E., Slijepčević, S., & Škrinjarić, B. (2021). Conceptual research framework of consumer resilience to privacy violation online. Sustainability, 13(3), 1238. doi:

https://doi.org/10.3390/su13031238

62. Budak, J., Rajh, E., & Škrinjarić, B. (2023). Resilience to online privacy violation: developing a typology of consumers. Scientific Annals of Economics and Business, 70(3), 379-398. doi: https://doi.org/10.47743/saeb2023-0028

63. Budak, J., Škrinjarić, B., & Rajh, E. (2022). Resilience to online privacy violation: The role of socio-demographic attributes. 8th REDETE Conference Researching Economic Development and Entrepreneurship in Transition Economies: Proceedings, 141–154. Banja Luka: Faculty of Economics, University of Banja Luka.

64. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 34(3), 523–548. doi: https://doi.org/10.2307/25750690

65. Butler, J. C. (2000). Personality and emotional correlates of right-wing authoritarianism. Social Behavior and Personality, 28(1), 1–14. doi: https://doi.org/10.2224/sbp.2000.28.1.1

66. Butler, L., Morland, L., & Leskin, G. (2007). Psychological resilience in the face of terrorism. Psychology of terrorism, 400-417.

67. Cai, Y., & Zhu, D. (2016). Fraud detections for online businesses: A perspective from blockchain technology. Financial Innovation, 2(1), 2–20. doi: https://doi.org/10.1186/s40854-016-0039-4

68. Callister, W. D., & Rethwisch, D. G. (2018). Materials science and engineering: An introduction (10th ed.). New York, NY: Wiley.

69. Calo, R. M. (2011). The boundaries of privacy harm. Indiana Law Journal, 86(3), 1131–1162.

70. Campbell, F. C. (2008). Elements of metallurgy and engineering alloys. ASM International. doi: https://doi.org/10.31399/asm.tb.emea.9781627082518

71. Campbell-Sills, L., Cohan, S. L., & Stein, M. B. (2006). Relationship of resilience to personality, coping, and psychiatric symptoms in young adults. Behaviour Research and Therapy, 44(4), 585–599. doi: https://doi.org/10.1016/j.brat.2005.05.001

72. Campbell-Sills, L., Forde, D. R., & Stein, M. B. (2009). Demographic and childhood environmental predictors of resilience in a community sample. Journal of Psychiatric Research, 43(12), 1007–1012. doi: https://doi.org/10.1016/j.jpsychires.2009.01.013

73. Carpenter, S., Walker, B., Anderies, J., & Abel, N. (2001). From metaphor to measurement: Resilience of what to what? Ecosystems, 4(8), 765–781. doi: https://doi.org/10.1007/s10021-001-0045-9

74. Carver, C. S., Scheier, M. F., & Segerstrom, S. C. (2010). Optimism. Clinical Psychology Review, 30(7), 879–889. doi: https://doi.org/10.1016/j.cpr.2010.01.006

75. Carver, C. S., Scheier, M. F., & Weintraub, J. K. (1989). Assessing coping strategies: A theoretically based approach. Journal of Personality and Social Psychology, 56(2), 267–283. doi: https://doi.org/10.1037/0022-3514.56.2.267

76. Carver, C. S., Smith, R. G., Antoni, M. H., Petronis, V. M., Weiss, S., & Derhagopian, R. P. (2005). Optimistic personality and psychosocial well-being during treatment predict psychosocial well-being among long-term survivors of breast cancer. Health Psychology, 24(5), 508–516. doi: https://doi.org/10.1037/0278-6133.24.5.508

77. Cerullo, V., & Cerullo, M. J. (2004). Business continuity planning: A comprehensive approach. Information Systems Management, 21(3), 70–78. doi: https://doi.org/10.1201/1078/44432.21.3.20040601/82480.11

78. Chang, C. E., Maydeu-Olivares, A., & D'Zurilla, T. J. (1997). Optimism and pessimism as partially independent constructs: Relations to positive and negative affectivity and psychological well-being. Personality and Individual Differences, 23(3), 433–440. doi: https://doi.org/10.1016/S0191-8869(97)80009-8

79. Chang, Y., Wong, S. F., Libaque-Saenz, C. F., & Lee, H. (2018). The role of privacy policy on consumers' perceived privacy. Government Information Quarterly, 35(3), 445–459. doi: https://doi.org/10.1016/j.giq.2018.04.002

80. Chellappa, R. K., & Pavlou, P. A. (2002). Perceived information security, financial liability and consumer trust in electronic commerce transactions. Logistics Information Management, 15(5/6), 358–368. doi: https://doi.org/10.1108/09576050210447046

81. Chen, E., & Miller, G. E. (2012). "Shift-and-persist" strategies: Why low socioeconomic status isn't always bad for health. Perspectives on Psychological Science, 7(2), 135–158. doi: https://doi.org/10.1177/1745691612436694

82. Chen, H. T., & Chen, W. (2015). Couldn't or wouldn't? The influence of privacy concerns and self-efficacy in privacy management on privacy protection. Cyberpsychology,

Behavior, and Social Networking, 18(1), 13–19. doi: https://doi.org/10.1089/cyber.2014.0456

83. Chen, K., & Rea, A. (2004). Protecting personal information online: A survey of user privacy concerns and control techniques. Journal of Computer Information Systems, 44(4), 85–92.

84. Chen, Y., Ramamurthy, K., & Wen, K.W. (2012). Organizations' information security policy compliance: Stick or carrot approach? Journal of Management Information Systems, 29(3), 157–188. doi: https://doi.org/10.2753/MIS0742-1222290305

85. Chiou, A. (2009). Cross cultural perceptions on privacy in the United States, Vietnam, Indonesia, and Taiwan. In K. Chen & A. Fadlalla (Eds.), Online consumer protection: Theories of human relativism (pp. 284–298). New York, NY: IGI Global. doi: https://doi.org/10.4018/978-1-60566-012-7.ch014

86. Cicchetti, D., & Garmezy, N. (1993). Prospects and promises in the study of resilience. Development and Psychopathology, 5(4), 497–502. doi: https://doi.org/10.1017/S0954579400006118

87. Clarke, R. (2009). Privacy impact assessment: Its origins and development. Computer Law and Security Review, 25(2), 123–135. doi: https://doi.org/10.1016/j.clsr.2009.02.002

88. Clauss-Ehlers, C. S. (2008). Sociocultural factors, resilience, and coping: Support for a culturally sensitive measure of resilience. Journal of Applied Developmental Psychology, 29(3), 197–212. doi: https://doi.org/10.1016/j.appdev.2008.02.004

89. Coles, E., & Buckle, P. (2004). Developing community resilience as a foundation for effective disaster recovery. The Australian Journal of Emergency Management, 19(4), 6–15.

90. Colwill, C. (2009). Human factors in information security: The insider threat – Who can you trust these days? Information Security Technical Report, 14(4), 186–196. doi: https://doi.org/10.1016/j.istr.2010.04.004

91. Connor, K. M., & Davidson, J. R. T. (2003). Development of a new resilience scale: The Connor-Davidson resilience scale (CD-RISC). Depression and Anxiety, 18(2), 76–82. doi: https://doi.org/10.1002/da.10113

92. Contissa, G., Lagioia, F., Lippi, M., Micklitz, H. W., Palka, P., Sartor, G., & Torroni, P. (2018). Towards consumer-empowering artificial intelligence. Proceedings of the Twenty-Seventh International Joint Conference on Artificial Intelligence: Evolution of the Contours of

AI, 5150–5157. doi: https://doi.org/10.24963/ijcai.2018/714

93. Costa, P. T., & McCrae, R. R. (1992). Normal personality assessment in clinical practice: The NEO Personality Inventory. Psychological assessment, 4(1), 5. doi: https://doi.org/10.1521/pedi.1992.6.4.343

94. Coutu, D. L. (2002). How resilience works. Harvard Business Review, 80(5), 46–56.

95. Cranor, L. F., Reagle, J., & Ackerman, M. S. (2000). Beyond concern: Understanding net users' attitudes about online privacy. In I. Vogelsang & B. M. Compaine (Eds.), The internet upheaval: Raising questions, seeking answers in communications policy (pp. 47–70). Cambridge, MA: MIT Press.

96. Crowcroft, J. (2015). On the duality of resilience and privacy. Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences, 471(2175), 1–6. doi: http://dx.doi.org/10.1098/rspa.2014.0862

97. Cummins, S., Peltier, J. W., Schibrowsky, J. A., & Nill, A. (2014). Consumer behavior in the online context. Journal of Research in Interactive Marketing 8(3), 169–202. doi: https://doi.org/10.1108/JRIM-04-2013-0019

98. Dalziell, E. P., & McManus, S. T. (2004). Resilience, vulnerability and adaptive capacity: Implications for system performance. International Forum for Engineering Decision Making (IFED), University of Canterbury, Christchurch.

99. Das, G., Jain, S. P., Maheswaran, D., Slotegraaf, R. J., & Srinivasan, R. (2021). Pandemics and marketing: Insights, impacts, and research opportunities. Journal of the Academy of Marketing Science, 49, 835–854. doi: https://doi.org/10.1007/s11747-021-00786-y

100. Davis, M. C., Luecken, L., & Lemery-Chalfant, K. (2009). Resilience in common life: Introduction to the special issue. Journal of Personality, 77, 1637–1644. doi: https://doi.org/10.1111/j.1467-6494.2009.00595.x

101. Davoudi, S., Shaw, K., Haider, L. J., Quinlan, A. E., Peterson, G. D., Wilkinson, C., … Davoudi, S. (2012). Resilience: A bridging concept or a dead end? "Reframing" resilience: Challenges for planning theory and practice. Interacting traps: Resilience assessment of a pasture management system in northern Afghanistan. Urban resilience: What does it mean in planning practice? Resilience as a useful concept for climate change adaptation? The

politics of resilience for planning: A cautionary note. Planning Theory & Practice, 13(2):299–333. doi: https://doi.org/10.1080/14649357.2012.677124

102. Davydov, D. M., Stewart, R., Ritchie, K., & Chaudieu, I. (2010). Resilience and mental health. Clinical Psychology Review, 30(5), 479–495. doi: https://doi.org/10.1016/j.cpr.2010.03.003

103. De Ryck, P., Nikiforakis, N., Desmet, L., & Joosen, W. (2013, May). Tabshots: Client-side detection of tabnabbing attacks. Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security, 447–456. doi: https://doi.org/10.1145/2484313.2484371

104. Deans, K., & Garry, T. (2013). Consumer resilience and the quest for alternate third places in post-quake Christchurch. Retrieved from: https://www.researchgate.net/profile/Tony-Garry-2/publication/256118024_Consumer_Resilience_and_the_Quest_for_Alternate_Third_Places_in_Post-Quake_Christchurch/links/55839c3408ae4738295b80c7/Consumer-Resilience-and-the-Quest-for-Alternate-Third-Places-in-Post-Quake-Christchurch.pdf

105. Demangeot, C., & Broderick, A. J. (2007). Conceptualising consumer behavior in online shopping environments. International Journal of Retail & Distribution Management, 35(11), 878–894. doi: https://doi.org/10.1108/09590550710828218

106. Dennis, C., Merrilees, B., Jayawardhena, C., & Wright, L. T. (2009). E-consumer behavior. European Journal of Marketing, 43(9/10), 1121–1139. doi: https://doi.org/10.1108/03090560910976393

107. Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. European Journal of Social Psychology, 45(3), 285–297. doi: https://doi.org/10.1002/ejsp.2049

108. Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents – measurement validity and a regression model. Behaviour & Information Technology, 23(6), 413–422. doi: https://doi.org/10.1144929041000171572 3

109. Dinev, T., & Hart, P. (2005). Internet privacy concerns and social awareness as determinants of intention to transact. International Journal of Electronic Commerce, 10(2), 7–29. doi: https://doi.org/10.2753/JEC1086-4415100201

110. Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce

transactions. Information Systems Research, 17(1), 61–80. doi: https://doi.org/10.1287/isre.1060.0080

111. Dobrolyubova, E., Klochkova, E., & Alexandrov, O. (2019). Digitalization and effective government: What is the cause and what is the effect? In D. Alexandrov, A. Boukhanovsky, A. Chugunov, Y. Kabanov, O. Koltsova, & I. Musabirov (Eds.), Digital transformation and global society. DTGS 2019. Communications in Computer and Information Science: Vol. 1038 (pp. 55–67). Cham: Springer. doi: https://doi.org/10.1007/978-3-030-37858-5_5

112. Dubbeldeman, R., & Ward S. (2015). Smart cities: How rapid advances in technology are reshaping our economy and society. Deloitte, The Netherlands. Retrieved from: https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/public-sector/deloitte-nl-ps-smart-cities-report.pdf

113. Duchek, S. (2020). Organizational resilience: A capability-based conceptualization. Business Research, 13(1), 215–246. doi: https://doi.org/10.1007/s40685-019-0085-7

114. Dyer, J. G., & McGuinness, T. M. (1996). Resilience: Analysis of the concept. Archives of Psychiatric Nursing, 10(5), 276–282. doi: https://doi.org/10.1016/S0883-9417(96)80036-7

115. Earvolino-Ramirez, M. (2007). Resilience: A concept analysis. Nursing Forum, 42(2), 73–82. doi: https://doi.org/10.1111/j.1744-6198.2007.00070.x

116. Egeland, B., Carlson, E., & Sroufe, L. (1993). Resilience as process. Development and Psychopathology, 5(4), 517–528. doi: ttps://doi.org/10.1017/S0954579400006131

117. Elmassah, S., & Hassanein, E. A. (2022). Digitalization and subjective wellbeing in Europe. Digital Policy, Regulation and Governance, 24(1), 52–73. doi: https://doi.org/10.1108/DPRG-05-2021-0060

118. Etzioni, A. (1999). The limits of privacy. New York, NY: Basic Books.

119. European Commission. (2011a). Attitudes on data protection and electronic identity in the European Union. Special Eurobarometer 359. Retrieved from: https://joinup.ec.europa.eu/sites/default/files/document/2014-12/Part%20I%20of%20Special%20Eurobarometer%20359%20-%20Attitudes%20on%20Data%20Protection%20and%20Electronic%20Identity%20in%20the%20European%20Union.pdf

120. European Commission. (2011b). Consumer empowerment in the EU. Commission Staff Working Paper.

121. European Commission. (2020). What is personal data? Retrieved from: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

122. European Commission & European Parliament, Brussels. (2019). Eurobarometer 91.1 (2019). GESIS data archive, Cologne. ZA7561 data file version 1.0.0. Retrieved from: https://search.gesis.org/research_data/ZA7561?doi=10.4232/1.14070

123. Eurostat. (2021). Digital economy and society statistics – households and individuals. Retrieved from: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_households_and_individuals

124. Everett, C. (2016). Ransomware: To pay or not to pay? Computer Fraud & Security, 2016(4), 8–12. doi: https://doi.org/10.1016/s1361-3723(16)30036-7

125. Ewen, R. B. (1998). Personality: A topical approach: Theories, research, major controversies, and emerging findings. Lawrence Erlbaum Associates Publishers.

126. Feng, Y., & Xie, W. (2014). Teens' concern for privacy when using social networking sites: An analysis of socialization agents and relationships with privacy-protecting behaviors. Computers in Human Behavior, 33, 153–162. doi: https://doi.org/10.1016/j.chb.2014.01.009

127. Ferrari, R. (2015). Writing narrative style literature reviews. Medical Writing, 24, 230–235. doi: https://doi.org/10.1179/2047480615Z.000000000329

128. Fiksel, J. (2003). Designing resilient, sustainable systems. Environmental Science and Technology, 37(23), 5330–5339. doi: https://doi.org/10.1021/es0344819

129. Flaherty, D. H. (1989). Protecting privacy in surveillance societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States. UNC Press Books.

130. Fletcher, D., & Fletcher, J. (2005). A meta-model of stress, emotions and performance: Conceptual foundations, theoretical framework, and research directions. Journal of Sports Sciences, 23, 157–158.

131. Fletcher, D., Hanton, S., & Mellalieu, S. D. (2006). An organizational stress review: Conceptual and theoretical issues in competitive sport. In S. Hanton & S. D. Mellalieu (Eds.), Literature reviews in sport psychology (pp. 321–374). Hauppauge, NY: Nova Science.

132. Fletcher, D., & Scott, M. (2010). Psychological stress in sports coaches: A review of concepts, theory and research. Journal of Sports Sciences, 28, 127–137. doi: https://doi.org/10.1080/02640410903406208

133. Folke, C., Carpenter, S., Elmqvist, T., Gunderson, L., Holling, C. S., Walker, B. … Svedin, U. (2002). Resilience and sustainable development: Building adaptive capacity in a world of transformations. Scientific background paper on resilience for the process of the World Summit on Sustainable Development on behalf of the Environmental Advisory Council to the Swedish Government.

134. Folke, C., Carpenter, S. R., Walker, B., Scheffer, M., Chapin, T., & Rockström, J. (2010). Resilience thinking: Integrating resilience, adaptability and transformability. Ecology and Society, 15(4), 20. doi: https://doi.org/10.5751/ES-03610-150420

135. Fredrickson, B. L. (2001). The role of positive emotions in positive psychology: The broaden-and-build theory of positive emotions. American Psychologist, 56(3), 218–226. doi: https://doi.org/10.1037/0003-066x.56.3.218

136. Friborg, O., Barlaug, D., Martinssen, M., Rosenvinge, J. H., & Hjemdal, O. (2005). Resilience in relation to personality and intelligence. International Journal of Methods in Psychiatric Research, 14, 29–42. doi: https://doi.org/10.1002/mpr.15

137. Friborg, O., Hjemdal, O., Rosenvinge, J. H., & Martinussen, M. (2003). A new rating scale for adult resilience: What are the central protective resources behind healthy adjustment? International Journal of Methods in Psychiatric Research, 12(2), 65–76. doi: https://doi.org/10.1002/mpr.143

138. Fuchs, C. (2012). The political economy of privacy on Facebook. Television and New Media, 13(2), 139–159. doi: https://doi.org/10.1177/1527476411415699

139. Furnell, S. M., & Karweni, T. (1999). Security implications of electronic commerce: A survey of consumers and businesses. Internet Research, 9(5), 372–382. doi: https://doi.org/10.1108/10662249910297778

140. Gallegos-Segovia, P. L., Bravo-Torres, J. F., Larios-Rosillo, V. M., Vintimilla-Tapia, P. E., Yuquilima-Albarado, I. F., & Jara-Saltos, J. D. (2017). Social engineering as an attack vector for ransomware. 2017 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON), 1–6. doi: https://doi.org/10.1109/chilecon.2017.8229528

141. Galli, N., & Vealey, R. S. (2008). "Bouncing back" from adversity: Athletes' experiences of resilience. The Sport Psychologist, 22(3), 316–335. doi: https://doi.org/10.1123/tsp.22.3.316

142. Gallopín, G. C. (2006). Linkages between vulnerability, resilience, and adaptive capacity. Global Environmental Change, 16(3), 293–303. doi: https://doi.org/10.1016/j.gloenvcha.2006.02.004

143. Ganor, M., & Ben-Lavy, Y. (2003). Community resilience: Lessons derived from Gilo under fire. Journal of Jewish Communal Service, 79(2/3), 105–108.

144. Garmezy, N. (1985). Stress-resistant children: The search for protective factors. In J. E. Stevenson (Ed.), Recent research in developmental psychopathology: Journal of Child Psychology and Psychiatry book supplement (pp. 213–233). Oxford: Pergamon Press.

145. Garmezy, N. (1987). Stress, competence, and development: Continuities in the study of schizophrenic adults, children vulnerable to psychopathology, and the search for stress-resistant children. American Journal of Orthopsychiatry, 57(2), 159–174. doi: https://doi.org/10.1111/j.1939-0025.1987.tb03526.x

146. Garmezy, N. (1991). Resiliency and vulnerability to adverse developmental outcomes associated with poverty. American Behavioral Scientist, 34(4), 416–430. doi: http://dx.doi.org/10.1177/0002764291034004003

147. Gazzola, P., Colombo, G., Pezzetti, R., & Nicolescu, L. (2017). Consumer empowerment in the digital economy: Availing sustainable purchasing decisions. Sustainability, 9(5), 693. doi: https://doi.org/10.3390/su9050693

148. Gellman, R., & Dixon, P. (2011). Online privacy: A reference handbook. Santa Barbara, CA: ABC Clio.

149. General Data Protection Regulation (GDPR). (2020). Retrieved from: https://gdpr.eu/eu-gdpr-personal-data/?cn-reloaded=1

150. Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. Computers & Security, 77, 226–261. doi: https://doi.org/10.1016/j.cose.2018.04.002

151. Gerbing, D. W., & Anderson, J. C. (1988). An updated paradigm for scale development incorporating unidimensionality and its assessment. Journal of Marketing Research, 25(2), 186–192. doi: https://doi.org/10.1177/002224378802500207

152. Ghafir, I., Prenosil, V., Alhejailan, A., & Hammoudeh, M. (2016, August). Social engineering attack strategies and defence approaches. 2016 IEEE 4th International

Conference on Future Internet of Things and Cloud (FiCloud), 145–149. doi: https://doi.org/10.1109/ficloud.2016.28

153. Gilgun, J. F. (2005). Evidence-based practice, descriptive research and the Resilience–Schema–Gender–Brain Functioning (RSGB) assessment. British Journal of Social Work, 35(6), 843–862. doi: https://doi.org/10.1093/bjsw/bch216

154. Ginosar, A., & Ariel, Y. (2017). An analytical framework for online privacy research: What is missing? Information & Management, 54(7), 948–957. doi: https://doi.org/10.1016/j.im.2017.02.004

155. Glasman, L. R., & Albarracín, D. (2006). Forming attitudes that predict future behavior: A meta-analysis of the attitude-behavior relation. Psychological Bulletin, 132(5), 778–822. doi: https://doi.org/10.1037/0033-2909.132.5.778

156. Godschalk, D. (2003). Urban hazard mitigation: Creating resilient cities. Natural Hazards Review, 4(3), 136–143. doi: https://doi.org/10.1061/(ASCE)1527-6988(2003)4:3(136)

157. Goldberg, L. R. (1993). The structure of phenotypic personality traits. American Psychologist, 48(1), 26–34. https://doi.org/10.1037/0003-066X.48.1.26

158. Goleman, D. (1997). Emotional intelligence. New York, NY: Bantam Books.

159. Goold, B. (2009). Surveillance and the political value of privacy. Amsterdam Law Forum, 1(4), 3–6. doi: https://doi.org/10.37974/ALF.80

160. Goold, B. (2010). How much surveillance is too much? Some thoughts on surveillance, democracy and the political value of privacy. In D. Schartum (Ed.), Surveillance in a constitutional government (pp. 38–48). Fakbokforlaget.

161. Gordon J. E., 1978, Structures, Penguin Books, Harmondsworth, UK.

162. Gotsch, M. L., & Schögel, M. (2023). Addressing the privacy paradox on the organizational level: Review and future directions. Management Review Quarterly, 73, 263–296. doi: https://doi.org/10.1007/s11301-021-00239-4

163. Graziano, W. G., & Eisenberg, N. (1997). Agreeableness: A dimension of personality. In R. Hogan, J. Johnson, & S. Briggs (Eds.), Handbook of personality psychology (pp. 794–825). San Diego, CA: Academic Press. doi: https://doi.org/10.1016/B978-012134645-4/50031-7

164. Graziano, W. G., Habashi, M. M., Sheese, B. E., & Tobin, R. M. (2007). Agreeableness, empathy, and helping: A person × situation perspective. Journal of Personality and Social

Psychology, 93(4), 583–599. doi: https://doi.org/10.1037/0022-3514.93.4.583

165. Green, B. N., Johnson, C. D., & Adams, A. (2006). Writing narrative literature reviews for peer-reviewed journals: Secrets of the trade. Journal of Chiropractic Medicine, 5(3), 101–117. doi: https://doi.org/10.1016/S0899-3467(07)60142-6

166. Greene, R. R. (2002). Holocaust survivors: A study in resilience. Journal of Gerontological Social Work, 37(1), 3–18. doi: https://doi.org/10.1300/J083v37n01_02

167. Gu, Q., & Day, C. (2007). Teachers' resilience: A necessary condition for effectiveness. Teaching and Teacher Education, 23(8), 1302–1316. doi: https://doi.org/10.1016/j.tate.2006.06.006

168. Gunderson, L. H. (2000). Ecological resilience–in theory and application. Annual Review of Ecology and Systematics, 31(1), 425–439. doi: https://doi.org/10.1146/annurev.ecolsys.31.1.425

169. Gunderson, L. H., & Holling, C. S. (Eds.). (2002). Panarchy: Understanding transformations in human and natural systems. Washington, DC: Island Press.

170. Gupta, S., Singhal, A., & Kapoor, A. (2016, April). A literature survey on social engineering attacks: Phishing attack. 2016 International Conference on Computing, Communication and Automation (ICCCA), 537–540. doi: https://doi.org/10.1109/ccaa.2016.7813778

171. Gurung, A., & Jain, A. (2009). Antecedents of online privacy protection behaviour: Towards an integrative model. In K. Chen & A. Fadlalla (Eds.), Online consumer protection: Theories of human relativism (pp. 151–190). New York; NY: IGI Global. doi: https://doi.org/10.4018/978-1-60566-012-7.ch007

172. Gwadz, M. V., Clatts, M. C., Yi, H., Leonard, N. R., Goldsamt, L., & Lankenau, S. (2006). Resilience among young men who have sex with men in New York City. Sexuality Research and Social Policy Journal of NSRC, 3(1), 13–21. doi: https://doi.org/10.1525/srsp.2006.3.1.13

173. Haimes, Y. Y. (2009). On the definition of resilience in systems. Risk Analysis: An International Journal, 29(4), 498–501. doi: https://doi.org/10.1111/j.1539-6924.2009.01216.x

174. Hair, J., Black, W., Babin, B., Anderson, R., & Tatham, R. (2006). Multivariate data analysis (6th ed.). Upper Saddle River, NJ: Pearson Prentice Hall.

175. Hair, J. F., Jr., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2021). A primer on partial

least squares structural equation modeling (PLS-SEM). Sage Publications.

176. Hargittai, E., & Dobransky, K. (2017). Old dogs, new clicks: Digital inequality in skills and uses among older adults. Canadian Journal of Communication, 42(2), 195–212. doi: https://doi.org/10.22230/cjc.2017v42n2a3176

177. Heppner, P., Cook, S. W., Wright, D. M., & Johnson, W. C. (1995). Progress in resolving problems: A problem-focused style of coping. Journal of Counseling Psychology, 42(3), 279–293. doi: https://doi.org/10.1037/0022-0167.42.3.279

178. Herrman, H., Stewart, D. E., Diaz-Granados, N., Berger, E. L., Jackson, B., & Yuen, T. (2011). What is resilience? The Canadian Journal of Psychiatry, 56(5), 258–265. doi: https://doi.org/10.1177/070674371105600504

179. Herrmann, D. S. (2007). Complete guide to security and privacy metrics: Measuring regulatory compliance, operational resilience, and ROI. Boca Ratan, FL: CRC Press. doi: https://doi.org/10.1201/9781420013283

180. Hettema, J. M., Neale, M. C., Myers, J. M., Prescott, C. A., & Kendler, K. S. (2006). A population-based twin study of the relationship between neuroticism and internalizing disorders. American Journal of Psychiatry, 163(5), 857–864. doi: https://doi.org/10.1176/ajp.2006.163.5.857

181. Hiller, J. S., & Blanke, J. M. (2017). Smart cities, big data and the resilience of privacy. Hastings Law Journal, 68(2), 309–356.

182. Hiller, J. S., & Russell, R. S. (2015). Modalities for cyber security and privacy resilience: The NIST approach. Proceedings of the ISCRAM 2015 Conference, Kristiansand. Retrieved from: https://idl.iscram.org/files/janineshiller/2015/1203_JanineS.Hiller+RobertaS.Russell2015.pdf

183. Hillman, C. H., Erickson, K. I., & Kramer, A. F. (2008). Be smart, exercise your heart: Exercise effects on brain and cognition. Nature Reviews Neuroscience, 9, 58–65. doi: https://doi.org/10.1038/nrn2298

184. Hind, P., Frost, M., & Rowley, S. (1996). The resilience audit and the psychological contract. Journal of Managerial Psychology, 11(7), 18–29. doi: https://doi.org/10.1108/02683949610148838

185. Hoffman, D., Novak, T. A., & Peralta, M. (1999). Building consumer trust online.

Communications of the ACM, 42(4), 80–85. doi: https://doi.org/10.1145/299157.299175

186. Holling, C. S. (1973). Resilience and stability of ecological systems. Annual Review of Ecological Systems, 4, 1–23. doi: https://doi.org/10.1146/annurev.es.04.110173.000245

187. Holling, C. S. (1996). Engineering resilience versus ecological resilience. In P. C. Schulze (Ed.), Engineering within ecological constraints (pp. 31–44). Washington, DC: National Academy Press.

188. Holling, C. S. (2001). Understanding the complexity of economic, ecological, and social systems. Ecosystems, 4, 390-405. doi: https://doi.org/10.1007/s10021-001-0101-5

189. Hollnagel, E. (2011). Prologue: The scope of resilience engineering. In E. Hollnagel, J. Pariès, D. D. Woods, & J. Wreathall (Eds.), Resilience engineering in practice: A guidebook (pp. xxix–xxxix). Surrey: Ashgate.

190. Hollnagel, E., Woods, D. D., & Leveson, N. (Eds.). (2006). Resilience engineering: Concepts and precepts. Ashgate Publishing, Ltd.

191. Hosseini, S., Barker, K., & Ramirez-Marquez, J. E. (2016). A review of definitions and measures of system resilience. Reliability Engineering & System Safety, 145, 47–61. doi: http://dx.doi.org/10.1016/j.ress.2015.08.006

192. Huelin, R., Iheanacho, I., Payne, K., & Sandman, K. (2015). What's in a name? Systematic and nonsystematic literature reviews, and why the distinction matters. The Evidence, 34–37.

193. Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. Information Security Technical Report, 13(4), 247–255. doi: https://doi.org/10.1016/j.istr.2008.10.010

194. Hwang, W., Jung, H. S., & Salvendy, G. (2006). Internationalisation of e-commerce: A comparison of online shopping preferences among Korean, Turkish and US populations. Behaviour & Information Technology, 25, 3–18. doi: https://doi.org/10.1080/01449290512331335636

195. Ijaz, S., Ali Shah, M., Khan, A., & Ahmed, M. (2016). Smart cities: A survey on security concerns. International Journal of Advanced Computer Science and Applications (IJACSA), 7(2), 612–625. doi: https://doi.org/10.14569/IJACSA.2016.070277

196. International Telecommunication Union. (2015). ICT facts and figures. Geneva:

International Telecommunication Union. Retrieved from: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf

197. Islam, S. (2019). Factors influencing customer's intention to adopt online shopping: A holistic approach. International Journal of Business and Technopreneurship, 9(1), 57–66.

198. ISO/IEC Standard No. 27001:2013 (ISO/IEC 27001:2013). Retrieved from: https://www.iso.org/standard/27001#lifecycle

199. ISO/IEC Standard No. 27002:2005 (ISO/IEC 27002:2005). Retrieved from: https://www.iso.org/standard/50297.html

200. Johnson, J., Gooding, A., Wood, A. M., & Tarrier, N. (2010). Resilience as positive coping appraisals: Testing the schematic appraisals model of suicide (SAMS). Behavior Research and Therapy, 48(3), 179–186. doi: http://dx.doi.org/10.1016/j.brat.2009.10.007

201. Jones, R., Raab, C., & Székely, I. (2018). Surveillance and resilience: Relationships, dynamics and consequences. Democracy and Security, 14(3), 238–275. doi: https://doi.org/10.1080/17419166.2017.1423472

202. Joseph, S., & Linley, A. (2006). Growth following adversity: Theoretical perspectives and implications for clinical practice. Clinical Psychology Review, 26(8), 1041–1053. doi: https://doi.org/10.1016/j.cpr.2005.12.006

203. Jost, J. T. (2006). The end of the end of ideology. American Psychologist, 61(7), 651–670. doi: https://doi.org/10.1037/0003-066X.61.7.651

204. Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014). Classification of security threats in information systems. Procedia Computer Science, 32, 489–496. doi: https://doi.org/10.1016/j.procs.2014.05.452

205. Joyce, M., & Kirakowski, J. (2015). Measuring attitudes towards the internet: The general internet attitude scale. International Journal of Human-Computer Interaction, 31(8), 506–517. doi: https://doi.org/10.1080/10447318.2015.1064657

206. Kaapu, T., & Tiainen, T. (2009). Consumers' views on privacy in e-commerce. Scandinavian Journal of Information Systems, 21(1), 1–20. Retrieved from: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1000&context=sjis

207. Kalniņš, R., Puriņš, J., & Alksnis, G. (2017). Security evaluation of wireless network access points. Applied Computer Systems, 21(1), 38–45. doi: https://doi.org/10.1515/acss-

2017-0005

208. Karabacak, B., & Sogukpinar, I. (2005). ISRAM: Information security risk analysis method. Computers & Security, 24(2), 147–159. doi: https://doi.org/10.1016/j.cose.2004.07.004

209. Kidd, S., & Shahar, G. (2008). Resilience in homeless youth: The key role of self-esteem. American Journal of Orthopsychiatry, 78(2), 163–172. doi: https://doi.org/10.1037/0002-9432.78.2.163

210. Kim, H., Yoo, D., Kang, J. S., & Yeom, Y. (2017, November). Dynamic ransomware protection using deterministic random bit generator. 2017 IEEE Conference on Application, Information and Network Security (AINS), 64–68. doi: https://doi.org/10.1109/ains.2017.8270426

211. Kimhi, S., & Shamai, M. (2004). Community resilience and the impact of stress: Adult response to Israel's withdrawal from Lebanon. Journal of Community Psychology, 32(4), 439–451. doi: https://doi.org/10.1002/jcop.20012

212. Klein, R. J. T., Nicholls, R. J., & Thomalla, F. (2003). Resilience to natural hazards: How useful is this concept? Global Environmental Change Part B: Environmental Hazards, 5(1), 35–45. doi: https://doi.org/10.1016/j.hazards.2004.02.001

213. Kline, R. B. (1998). Principles and practice of structural equation modeling. New York, NY: The Guilford Press.

214. Kocalevent, R. D., Berg, L., Beutel, M. E., Hinz, A., Zenger, M., Härter, M., ... Brähler, E. (2018). Social support in the general population: Standardization of the Oslo social support scale (OSSS-3). BMC Psychology, 6, 31. doi: https://doi.org/10.1186/s40359-018-0249-9

215. Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & Security, 64, 122–134. doi: https://doi.org/10.1016/j.cose.2015.07.002

216. Kotzé, M., & Nel, P. (2013). Psychometric properties of the adult resilience indicator. SA Journal of Industrial Psychology, 39(2), 1132. doi: http://dx.doi.org/10.4102/sajip.v39i2.1132

217. Kumaraguru, P., & Cranor, L. (2006). Privacy in India: Attitudes and awareness. In I. Goldberg & M. Atallah (Eds.), Privacy enhancing technologies (pp. 243–258). Berlin, Heidelberg: Springer. doi: https://doi.org/10.1007/11767831_16

218. Kursan Milaković, I. (2021). Purchase experience during the COVID-19 pandemic and

social cognitive theory: The relevance of consumer vulnerability, resilience, and adaptability for purchase satisfaction and repurchase. International Journal of Consumer Studies, 45(6), 1425–1442. doi: https://doi.org/10.1111/ijcs.12672

219. Ledesma, J. (2014). Conceptual frameworks and research models on resilience in leadership. Sage Open, 4(3), 1–8. doi: http://dx.doi.org/10.1177/2158244014545464

220. Lee, P. M. (2002). Behavioral model of online purchasers in e-commerce environment. Electronic Commerce Research, 2, 75–85. doi: https://doi.org/10.1023/A:1013340118965

221. Lee, H. H., & Cranford, J. A. (2008). Does resilience moderate the associations between parental problem drinking and adolescents' internalizing and externalizing behaviors?: A study of Korean adolescents. Drug and alcohol Dependence, 96(3), 213-221. doi: https://doi.org/10.1016/j.drugalcdep.2008.03.007

222. Lehdonvirta, V. (2012). A history of the digitalization of consumer culture: From Amazon through Pirate Bay to Farmville. In J. Denegri-Knott & M. Molesworth (Eds.), Digital virtual consumption (pp. 11–28). New York, NY: Routledge.

223. Leipold, B., & Greve, W. (2009). Resilience: A conceptual bridge between coping and development. European Psychologist, 14(1), 40-50. doi: https://doi.org/10.1027/1016-9040.14.1.40

224. Lengnick-Hall, C. A., Beck, T. E., & Lengnick-Hall, M. L. (2011). Developing a capacity for organizational resilience through strategic human resource management. Human Resource Management Review, 21(3), 243–255. doi: https://doi.org/10.1016/j.hrmr.2010.07.001

225. Lentzos, F., & Rose, N. (2009). Governing insecurity: Contingency planning, protection, resilience. Economy and Society, 38(2), 230–254. doi: http://dx.doi.org/10.1080/03085140902786611

226. Letzring, T. D., Block, J., & Funder, D. C. (2005). Ego-control and ego-resilience: Generalization of self-report scales based on personality descriptions from acquaintances, clinicians and the self. Journal of Research in Personality, 39(4), 395–422. doi: https://doi.org/10.1016/j.jrp.2004.06.003

227. Liao, C., Liu, C.-C., & Chen, K. (2011). Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: An integrated model. Electronic Commerce Research and Applications, 10(6), 702–715. doi: https://doi.org/10.1016/j.elerap.2011.07.003

228. Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Kott, A. (2013). Resilience metrics for cyber systems. Environment Systems and Decisions, 33(4), 471–476. doi: https://doi.org/10.1007/s10669-013-9485-y

229. Linnenluecke, M. K., & Griffiths, A. (2010). Beyond adaptation: Resilience for business in light of climate change and weather extremes. Business & Society, 49(3), 477–511. doi: https://doi.org/10.1177/0007650310368814

230. Linsner, S., Kuntke, F., Steinbrink, E., Franken, J., & Reuter, C. (2021). The role of privacy in digitalization – Analyzing perspectives of German farmers. Proceedings on Privacy Enhancing Technologies, 2021(3), 334–350. doi: https://doi.org/10.2478/popets-2021-0050

231. Longstaff, P. H. (2005). Security, resilience and communication in unpredictable environments such as terrorism, natural disasters and complex technology. Syracuse, NY: Author.

232. Longstaff, P. H., Koslowski, T. G., & Geoghegan, W. (2013). Translating resilience: A framework to enhance communication and implementation. Proceedings: 5th Symposium on Resilience Engineering: Managing Trade-offs, 1–10. Sophia Antipolis, France: Resilience Engineering Association. Retrieved from: http://publications.tno.nl/publication/34613515/X0B0iX/herrera-2014-resilience.pdf

233. Lorenz, D. (2013). The diversity of resilience: Contributions from a social science perspective. Natural Hazards, 67(1), 7-24. doi: https://doi.org/10.1007/s11069-010-9654-y

234. Lundberg, J., & Johansson, B. J. E. (2015). Systemic resilience model. Reliability Engineering & System Safety, 141, 22–32. doi: http://dx.doi.org/10.1016/j.ress.2015.03.013

235. Luthans, F. (2002). The need for and meaning of positive organizational behavior. Journal of Organizational Behavior, 23(6), 695–706. doi: https://doi.org/10.1002/job.165

236. Luthans, F., Vogelgesang, G. R., & Lester: B. (2006). Developing the psychological capital of resilience. Human Resource Development Review, 5(1), 25–44. doi: https://doi.org/10.1177/1534484305285335:

237. Luthar, S. S. (2006). Resilience in development: A synthesis of research across five decades. In D. Cicchetti & D. Cohen (Eds.), Developmental psychopathology: Risk, disorder, and adaptation (pp. 739–795). New York, NY: Wiley. doi: https://doi.org/10.1002/9780470939406.ch20

238. Luthar, S. S., & Cicchetti, D. (2000). The construct of resilience: Implications for interventions and social policies. Development and Psychopathology, 12(4), 857–885. doi: https://doi.org/10.1017/S0954579400004156

239. Luthar, S. S., Cicchetti, D., & Becker, B. (2000). The construct of resilience: A critical evaluation and guidelines for future work. Child Development, 71(3), 543–562. doi: http://dx.doi.org/10.1111/1467-8624.00164

240. Lwin, M., Wirtz, J., & Williams, J. D. (2007). Consumer online privacy concerns and responses: A power–responsibility equilibrium perspective. Journal of the Academy of Marketing Science, 35, 572–585. doi: https://doi.org/10.1007/s11747-006-0003-3

241. Madni, A. M., & Jackson, S. (2009). Towards a conceptual framework for resilience engineering. IEEE Systems Journal, 3(2), 181–191. doi: https://doi.org/10.1109/JSYST.2009.2017397

242. Mahoney, J. L., & Bergman, L. R. (2002). Conceptual and methodological considerations in a developmental approach to the study of positive adaptation. Journal of Applied Developmental Psychology, 23(2), 195–217. doi: https://doi.org/10.1016/S0193-3973(02)00104-1

243. Maio, G. R., Esses, V. M., & Bell, D. W. (2000). Examining conflict between components of attitudes: Ambivalence and inconsistency are distinct constructs. Canadian Journal of Behavioural Science / Revue canadienne des sciences du comportement, 32(2), 71–83. doi: https://doi.org/10.1037/h0087102

244. Major, B., Richards, C., Cooper, M. L., Cozzarelli, C., & Zubek, J. (1998). Personal resilience, cognitive appraisals and coping: An integrative model of adjustment to abortion. Journal of Personality and Social Psychology, 74(3), 735–752. doi: https://doi.org/10.1037/0022-3514.74.3.735

245. Malhotra, N., Kim, S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale and a causal model. Information System Research, 15(4), 336–355. doi: https://doi.org/10.1287/isre.1040.0032

246. Mallak, L. (1998). Putting organizational resilience to work. Industrial Management, 40, 8–13.

247. Mansfield, C. F., Beltman, S., Price, A., & McConney, A. (2012). "Don't sweat the small

stuff:" Understanding teacher resilience at the chalkface. Teaching and Teacher Education, 28(3), 357–367. doi: https://doi.org/10.1016/j.tate.2011.11.001

248. Manyena, S. B. (2006). The concept of resilience revisited. Disasters, 30(4), 434–450. doi: https://doi.org/10.1111/j.0361-3666.2006.00331.x

249. Markos, E., Labrecque, L. I., & Milne, G. R. (2012). Web 2.0 and consumers' digital footprint: Managing privacy and disclosure choices in social media. In A. G. Close (Ed.), Online consumer behavior: Theory and research in social media, advertising and e-tail (pp. 157–182). New York, NY: Routledge.

250. Martin-Breen, P., & Anderies, J. M. (2011). Resilience: A literature review. Brighton: Institute of Development Studies (IDS).

251. Martins, J. M., Yusuf, F., & Swanson, D. A. (2012). Consumer demographics and behaviour: Markets are people (Vol. 30). Springer Science & Business Media. doi: https://doi.org/10.1007/978-94-007-1855-5

252. Masten, A. S. (2001). Ordinary magic: Resilience processes in development. American Psychologist, 56(3), 227–238. doi: https://doi.org/10.1037/0003-066X.56.3.227

253. Masten, A. S., Best, K. M., & Garmezy, N. (1990). Resilience and development: Contributions from the study of children who overcome adversity. Development and Psychopathology, 2(4), 425–444. doi: https://doi.org/10.1017/S0954579400005812

254. Masten, A. S., & Coatsworth, J. (1998). The development of competence in favorable and unfavorable environments: Lessons from research on successful children. American Psychologist, 53(2), 205–220. doi: https://doi.org/10.1037/0003-066X.53.2.205

255. Masten, A. S., & Obradovic, J. (2007). Disaster preparation and recovery: Lessons from research on resilience in human development. Ecology and Society, 13(1), 9. doi: https://doi.org/10.5751/ES-02282-130109

256. Matthews, G., & Deary, I. J. (1998). Personality traits. Cambridge University Press.

257. McCrae, R. R. (1996). Integrating the levels of personality. Psychological Inquiry, 7(4), 353–356. doi: https://doi.org/10.1207/s15327965pli0704_10

258. McCrae, R. R., & Costa, P. T. (1986). Personality, coping, and coping effectiveness in an adult sample. Journal of Personality, 54(2), 385–404. doi: https://doi.org/10.1111/j.1467-6494.1986.tb00401.x

259. McCrae, R. R., & Costa, P. T. (1987). Validation of the five-factor model of personality across instruments and observers. Journal of Personality and Social Psychology, 52(1), 81–90. doi: https://doi.org/10.1037/0022-3514.52.1.81

260. McCrae, R. R., & John, O. P. (1992). An introduction to the five-factor model and its applications. Journal of Personality, 60(2), 175–215. doi: https://doi.org/10.1111/j.1467-6494.1992.tb00970.x

261. McCubbin, L. (2001, August). Challenges to the definition of resilience. Paper presented at the 109th Annual Meeting of the American Psychological Association, San Francisco, CA. Retrieved from https://files.eric.ed.gov/fulltext/ED458498.pdf

262. McDougall, R. (2015). Reviewing literature in bioethics research: Increasing rigour in non-systematic reviews. Bioethics, 29(7), 523–528. doi: https://doi.org/10.1111/bioe.12149

263. Milne, G. R., Rohm, A. J., & Bahl, S. (2004). Consumers' protection of online privacy and identity. Journal of Consumer Affairs, 38(2), 217–232. doi: https://doi.org/10.1111/j.1745-6606.2004.tb00865.x

264. Miyazaki, A., & Fernandez, A. (2001). Consumer perceptions of privacy and security risks for online shopping. The Journal of Consumer Affairs, 35(1), 27–44. doi: https://doi.org/10.1111/j.1745-6606.2001.tb00101.x

265. Moore, R. S., Moore, M. L., Shanahan, K. J., & Mack, B. (2015). Creepy marketing: Three dimensions of perceived excessive online privacy violation. Marketing Management, 25(1), 42–53.

266. Moschis, G. P. (2007). Stress and consumer behavior. Journal of the Academy of Marketing Science, 35, 430–444. doi: https://doi.org/10.1007/s11747-007-0035-3

267. Mosco, V. (2017). Citizenship in a post-internet world. In V. Mosco (Ed.), Becoming digital (pp. 175–212). Emerald Publishing Limited. doi: https://doi.org/10.1108/978-1-78743-295-620181006

268. Naef, M., & Schupp, J. (2009). Measuring trust: Experiments and surveys in contrast and combination. IZA Discussion Paper No. 4087. Bonn: Institute for the Study of Labor (IZA). doi: https://dx.doi.org/10.2139/ssrn.1367375

269. Nakaya, M., Oshio, A., & Kaneko, H. (2006). Correlations for adolescent resilience scale with big five personality traits. Psychological Reports, 98(3), 927–930. doi: https://doi.

org/10.2466/pr0.98.3.927-930

270. Nathan, A. J. (2016). China's changing of the guard: Authoritarian resilience. In K. E. Brodsgaard (Ed.), Critical readings on the Communist Party of China (pp. 86–99). Brill. doi: https://doi.org/10.1163/9789004302488_005

271. National Institute of Standards and Technology (NIST). (2012). NIST SP 800-30 Rev. 1: Guide for conducting risk assessments. Retrieved from: https://csrc.nist.gov/pubs/sp/800/30/r1/final

272. Nemeth, C. P. (2009). The ability to adapt. In C. P. Nemeth, E. Hollnagel, & S. Dekker (Eds.), Resilience engineering perspectives 2: Preparation and restoration (pp. 1–12). Farnham: Ashgate.

273. Norberg, P. A., Horne, D. R., Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. Journal of Consumer Affairs, 41(1), 100–126. doi: https://doi.org/10.1111/j.1745-6606.2006.00070.x

274. Norris, F., Stevens, S., Pfefferbaum, B., Wyche, K., & Pfefferbaum, R. (2008). Community resilience as a metaphor, theory, set of capacities, and strategy for disaster readiness. American Journal of Community Psychology, 41(1–2), 127–150. doi: https://doi.org/10.1007/s10464-007-9156-6

275. Oliveira, M. G., & Toaldo, A. M. M. (2015). New times, new strategies: Proposal for an additional dimension to the 4 P's for e-commerce dot-com. Journal of Information Systems and Technology Management, 12(1), 107–124. doi: https://doi.org/10.4301/S1807-17752015000100006

276. Ollier-Malaterre, A. (2009). Contributions of work—life and resilience initiatives to the individual/organization relationship. Human Relations, 63(1), 41–62. doi: https://doi.org/10.1177/0018726709342458

277. Olsson, C. A., Bond, L., Burns, J. M., Vella-Brodrick, D. A., & Sawyer, S. M. (2003). Adolescent resilience: A concept analysis. Journal of Adolescence, 26(1), 1–11. doi: https://doi.org/10.1016/S0140-1971(02)00118-5

278. Omer, M., Mostashari, A., & Lindemann, U. (2014). Resilience analysis of soft infrastructure systems. Procedia Computer Science, 28, 873–882. doi: https://doi.org/10.1016/j.procs.2014.03.104

279. Ong, A. D., Bergeman, C. S., Bisconti, T. L., & Wallace, K. A. (2006). Psychological resilience, positive emotions, and successful adaptation to stress in later life. Journal of Personality and Social Psychology, 91(4), 730–749. doi: https://doi.org/10.1037/0022-3514.91.4.730

280. Open Web Application Security Project (OWASP). (2022). OWASP risk rating methodology. Retrieved from: www.owas.org

281. Pachauri, M. (2001). Consumer behavior: A literature review. The Marketing Review, 2(3), 319–355. doi: https://doi.org/10.1362/1469347012569896

282. Panzarella, C., Alloy, L., & Whitehouse, W. (2006). Expanded hopelessness theory of depression: On the mechanisms by which social support protects against depression. Cognitive Therapy and Research, 30, 307–333. doi: https://doi.org/10.1007/s10608-006-9048-3

283. Parviainen, P., Tihinen, M., Kääriäinen, J., & Teppola, S. (2017). Tackling the digitalization challenge: How to benefit from digitalization in practice. International Journal of Information Systems and Project Management, 5(1), 63–77. doi: https://doi.org/10.12821/ijispm050104

284. Patterson, E. S., Woods, D. D., Roth, E. M., Cook, R. I., Wears, R. L., & Render, M. L. (2006). Three key levers for achieving resilience in medication delivery with information technology. Journal of Patient Safety, 2(1), 33–38.

285. Pauxtis, A. (2009). Google: Technological convenience vs. technological intrusion. In K. Chen & A. Fadlalla (Eds.), Online consumer protection: Theories of human relativism (pp. 1–16). London: IGI Global. doi: https://doi.org/10.4018/978-1-60566-012-7.ch001

286. Pavlou, A., & Fygenson, M. (2006). Understanding and predicting electronic commerce adoption: An extension of the theory of planned behavior. MIS Quarterly 30(1), 115–143. doi: https://doi.org/10.2307/25148720

287. Paton, D., Smith, L., & Violanti, J. (2000). Disaster response: risk, vulnerability and resilience. Disaster Prevention and Management: An International Journal, 9(3), 173-180. doi: https://doi.org/10.1108/09653560010335068

288. Paton, D., Smith, L., & Johnston, D. (2000). Volcanic hazards: risk perception and preparedness. New Zealand Journal of Psychology, 29(2), 86-91. Retreived from: https://

www.psychology.org.nz/journal-archive/NZJP-Vol292-2000-6-Paton.pdf

289. Peltier, T. R. (2005). Information security risk analysis. CRC Press. doi: https://doi.org/10.1201/9781420031195

290. Penner, L. A., Fritzsche, B. A., Craiger, J. P., & Freifeld, T. S. (1995). Measuring the prosocial personality. In J. N. Butcher & C. D. Spielberger (Eds.), Advances in personality assessment (Vol. 10, pp. 147–163). Lawrence Erlbaum Associates, Inc.

291. Peotta, L., Holtz, M. D., David, B. M., Deus, F. G., & Sousa, R. T. (2011). A formal classification of internet banking attacks and vulnerabilities. International Journal of Computer Science and Information Technology, 3(1), 186–197. doi: https://doi.org/10.5121/ijcsit.2011.3113

292. Perrings, C. (2006). Resilience and sustainable development. Environment and Development Economics, 11(4), 417–427. doi: https://doi.org/10.1017/S1355770X06003020

293. Pfefferbaum, B. J., Devoe, E. R., Stuber, J., Schiff, M., Klein, T. P., & Fairbrother, G. (2005). Psychological impact of terrorism on children and families in the United States. Journal of aggression, maltreatment & trauma, 9(3-4), 305-317. doi: https://doi.org/10.1300/J146v09n03_01

294. Pompon, R. (2016). IT security risk control management: An audit preparation plan. Apress. doi: https://doi.org/10.1007/978-1-4842-2140-2

295. Ponomarov, S. Y., & Holcomb, M. C. (2009). Understanding the concept of supply chain resilience. The International Journal of Logistics Management, 20(1), 124–143. doi: https://doi.org/10.1108/09574090910954873

296. Raab, C., & Goold, B. (2011). Protecting information privacy. Equality and Human Rights Commission Research Report No. 69. Retrieved from: https://ssrn.com/abstract=1967198

297. Raab, C. D., Jones, R., & Székely, I. (2015). Surveillance and resilience in theory and practice. Media and Communication, 3(2), 21–41. doi: https://doi.org/10.17645/mac.v3i2.220

298. Rabari, C., & Storper, M. (2015). The digital skin of cities: Urban theory and research in the age of the sensored and metered city, ubiquitous computing and big data. Cambridge Journal of Regions, Economy and Society, 8(1), 27–42. doi: https://doi.org/10.1093/cjres/rsu021

299. Rajh, E., Škrinjarić, B., & Budak, J. (2021). Otpornost potrošača na narušavanje online privatnosti: Testiranje mjerne ljestvice. Ekonomska misao i praksa / Economic Thought and Practice, 30(2), 527–544. doi: https://doi.org/10.17818/EMIP/2021/2.11

300. Rammstedt, B., & Oliver, J. P. (2007). Measuring personality in one minute or less: A 10-item short version of the big five inventory in English and German. Journal of Research in Personality, 41(1), 203–212. doi: https://doi.org/10.1016/j.jrp.2006.02.001

301. Reed, T. (2014). Digitized lives: Culture, power and social change in the internet era. New York and London: Taylor and Francis; Routledge. doi: https://doi.org/10.4324/9780203374672

302. Reich, J. W. (2006). Three psychological principles of resilience in natural disasters. Disaster Prevention and Management, 15(5), 793–798. doi: https://doi.org/10.1108/09653560610712739

303. Rew, D., & Minor, M. (2018). Consumer resilience and consumer attitude towards traumatic events. Journal of Customer Behaviour, 17(4), 319–334. doi: https://doi.org/10.1362/147539218X15445233217832

304. Rice, R. E. (2006). Influences, usage, and outcomes of internet health information searching: Multivariate results from the Pew surveys. International Journal of Medical Informatics, 75(1), 8–28. doi: https://doi.org/10.1016/j.ijmedinf.2005.07.032

305. Richard, M. O., Chebat, J. C., Yang, Z., & Putrevu, S. (2010). A proposed model of online consumer behavior: Assessing the role of gender. Journal of Business Research, 63(9–10), 926–934. doi: https://doi.org/10.1016/j.jbusres.2009.02.027

306. Richardson, G. E. (2002). The metatheory of resilience and resilience. Journal of Clinical Psychology, 58(3), 307–321. doi: https://doi.org/10.1002/jclp.10020

307. Roberts, E., Beel, D., Philip, L., & Townsend, L. (2017). Rural resilience in a digital society: Editorial. Journal of Rural Studies, 54, 355–359. doi: https://doi.org/10.1016/j.jrurstud.2017.06.010

308. Robins, R. W., Hendin, H. M., & Trzesniewski, K. H. (2001). Measuring global self-esteem: Construct validation of a single-item measure and the Rosenberg self-esteem scale. Personality and Social Psychology Bulletin, 27(2), 151–161. doi: https://doi.org/10.1177/0146167201272002

309. Rohmeyer, P., & Bayuk, J. L. (2019). How do I manage this? In P. Rohmeyer &

J. L. Bayuk, Financial cybersecurity risk management: Leadership perspectives and guidance for systems and institutions (pp. 125–156). Berkeley, CA: Apress. doi: https://doi.org/10.1007/978-1-4842-4194-3_6

310. Rosin, A. F., Proksch, D., Stubner, S., & Pinkwart, A. (2020). Digital new ventures: Assessing the benefits of digitalization in entrepreneurship. Journal of Small Business Strategy, 30(2), 59–71.

311. Rumgay, J. (2004). Scripts for safer survival: Pathways out of female crime. The Howard Journal of Criminal Justice, 43(4), 405–419. doi: https://doi.org/10.1111/j.1468-2311.2004.00338.x

312. Rutter, M. (1981). Stress, coping and development: Some issues and some questions. Journal of Child Psychology and Psychiatry and Allied Disciplines, 22, 323–356. doi: https://doi.org/10.1111/j.1469-7610.1981.tb00560.x

313. Rutter, M. (1987). Psychosocial resilience and protective mechanisms. American Journal of Orthopsychiatry, 57(3), 316–331. doi: https://doi.org/10.1111/j.1939-0025.1987.tb03541.x

314. Rutter, M. (2006). Implications of resilience concepts for scientific understanding. Annals of the New York Academy of Sciences, 1094(1), 1–12. doi: https://doi.org/10.1196/annals.1376.002

315. Sabbagh, K., Friedrich, R., El-Darwiche, B., Singh, M., Ganediwalla, S., & Katz, R. (2012). Maximizing the impact of digitization. The Global Information Technology Report, 2012, 121–133.

316. Salgado, J. F. (1997). The five factor model of personality and job performance in the European Community. Journal of Applied Psychology, 82(1), 30–43. doi: https://doi.org/10.1037/0021-9010.82.1.30

317. Salgado, J. F., Moscoso, S., & Lado, M. (2003). Evidence of cross-cultural invariance of the big five personality dimensions in work settings. European Journal of Personality, 17(1), 67–76. doi: https://doi.org/10.1002/per.482

318. Sarika, S., & Paul, V. (2015). AgentTab: An agent based approach to detect tabnabbing attack. Procedia Computer Science, 46, 574–581. doi: https://doi.org/10.1016/j.procs.2015.02.094

319. Saurwein, F., Just, N., & Latzer, M. (2015). Governance of algorithms: Options and limitations. Info, 17(6), 35–49. doi: https://doi.org/10.1108/info-05-2015-0025

320. Schaffers, H., Komninos, N., Pallot, M., Trousse, B., Nilsson, M., & Oliveira, A. (2011). Smart cities and the future internet: Towards cooperation frameworks for open innovation. In J. Domingue et al. (Eds.), The future internet: FIA 2011, LNCS 6656 (pp. 431–446). Berlin, Heidelberg: Springer. doi: https://doi.org/10.1007/978-3-642-20898-0_31

321. Schlosser, A. E., Shavitt, S., & Kanfer, A. (1999). Survey of internet users' attitudes toward internet advertising. Journal of Interactive Marketing, 13(3), 34–54. doi: https://doi.org/10.1002/(SICI)1520-6653(199922)13:3<34::AID-DIR3>3.0.CO;2-R

322. Schwarzer, R., Bäßler, J., Kwiatek, P., Schröder, K., & Zhang, J. X. (1997). The assessment of optimistic self-beliefs: Comparison of the German, Spanish, and Chinese versions of the general self-efficacy scale. Applied Psychology: An International Review, 46(1), 69–88. doi: https://doi.org/10.1111/j.1464-0597.1997.tb01096.x

323. Schwarzer, R., & Jerusalem, M. (1995). Generalised self-efficacy scale. In J. Weinman, S. Wright, & M. Johnston (Eds.), Measures in health psychology: A user's portfolio. Causal and control beliefs (pp. 35–37). Windsor: Nfer-Nelson.

324. Scully, D., Kremer, J., Meade, M. M., Graham, R., & Dudgeon, K. (1998). Physical exercise and psychological well-being: A critical review. British Journal of Sports Medicine, 32, 111–120. doi: https://doi.org/10.1136/bjsm.32.2.111

325. Seville, E., Brunsdon, D., Dantas, A., Le Masurier, J., Wilkinson, S., & Vargo, J. (2006). Building organisational resilience: A summary of key research findings. University of Canterbury Repository. Retrieved from: https://www.academia.edu/1028912/Building_organisational_resilience_A_summary_of_key_research_findings

326. Sharif, M. S., Shao, B., Xiao, F., & Saif, M. K. (2014). The impact of psychological factors on consumers trust in adoption of m-commerce. International Business Research, 7(5), 148–155. doi: https://doi.org/10.5539/ibr.v7n5p148

327. Sherer, M., Maddux, J. E., Mercandante, B., Prentice-Dunn, S., Jacobs, B., & Rogers, R. W. (1982). The self-efficacy scale: Construction and validation. Psychological Reports, 51(2), 663–671. doi: https://doi.org/10.2466/pr0.1982.51.2.663

328. Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to

information security policies: An exploratory field study. Information & Management, 51(2), 217–224. doi: https://doi.org/10.1016/j.im.2013.08.006

329. Sittig, D., & Singh, H. (2016). A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks. Applied Clinical Informatics, 7(2), 624–632. doi: https://doi.org/10.4338/aci-2016-04-soa-0064

330. Skinner, E. A., & Zimmer-Gembeck, M. J. (2007). The development of coping. Annual Review of Psychology, 58(1), 119–144. doi: https://doi.org/10.1146/annurev.psych.58.110405.085705

331. Smith, B. W., Dalen, J., Wiggins, K., Tooley, E., Christopher, P., & Bernard, J. (2008). The brief resilience scale: Assessing the ability to bounce back. International Journal of Behavioral Medicine, 15(3), 194–200. doi: https://doi.org/10.1080/10705500802222972

332. Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. MIS Quarterly, 35(4), 989–1015. doi: https://doi.org/10.2307/41409970

333. Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organisational practices. MIS Quarterly, 20(2), 167–196. doi: https://doi.org/10.2307/249477

334. Smith, J., Hewitt, B., & Skrbiš, Z. (2015). Digital socialization: Young people's changing value orientations towards internet use between adolescence and early adulthood. Information, Communication and Society, 18(9), 1022–1038. doi: https://doi.org/10.1080/1369118X.2015.1007074

335. Smith, P., Hutchison, D., Sterbenz, J. P., Schöller, M., Fessi, A., Karaliopoulos, M., Lac, C., & Plattner, B. (2011). Network resilience: A systematic approach. IEEE Communications Magazine, 49(7), 88–97. doi: https://doi.org/10.1109/MCOM.2011.5936160

336. Snyder, C. R. (Ed.). (2000). Handbook of hope: Theory, measures, and applications. Academic Press.

337. Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. Journal of Business Research, 104, 333–339. doi: https://doi.org/10.1016/j.jbusres.2019.07.039

338. Soanes, C., & Stevenson, A. (2006). Oxford dictionary of English (2nd ed.). Oxford: Oxford University Press.

339. Solomon, M. R., Bamossy, G. J., Askegaard, S. T., & Hogg, M. K. (2013). Consumer behavior: A European perspective (5th ed.). Harlow: Pearson.

340. Solove, D. J. (2006). A taxonomy of privacy. University of Pennsylvania Law Review, 154(3), 477–564. doi: https://doi.org/10.2307/40041279

341. Solove, D. J. (2008). Understanding privacy. Harvard: Harvard University Press.

342. Sonn, C. C., & Fisher, A. T. (1998). Sense of community: Community resilient responses to oppression and change. Journal of community psychology, 26(5), 457-472. doi: https://doi.org/10.1002/(SICI)1520-6629(199809)26:5<457::AID-JCOP5>3.0.CO;2-O

343. Soopramanien, D. (2011). Conflicting attitudes and scepticism towards online shopping: The role of experience. International Journal of Consumer Studies, 35(3), 338–347. doi: https://doi.org/10.1111/j.1470-6431.2010.00945.x

344. Southwick, S. M., Bonanno, G. A., Masten, A. S., Panter-Brick, C., & Yehuda, R. (2014). Resilience definitions, theory, and challenges: Interdisciplinary perspectives. European Journal of Psychotraumatology, 5, 25338. doi: http://dx.doi.org/10.3402/ejpt.v5.25338

345. Steen, R., & Aven, T. (2011). A risk perspective suitable for resilience engineering. Safety Science, 49(2), 292–297. doi: https://doi.org/10.1016/j.ssci.2010.09.003

346. Sterk, M., van de Leemput, I. A., & Peeters, E. T. (2017). How to conceptualize and operationalize resilience in socio-ecological systems? Current Opinion in Environmental Sustainability, 28, 108–113. doi: https://doi.org/10.1016/j.cosust.2017.09.003

347. Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. Information Systems Research, 13(1), 36–49. doi: https://doi.org/10.1287/isre.13.1.36.97

348. Strunz, S. (2012). Is conceptual vagueness an asset? Arguments from philosophy of science applied to the concept of resilience. Ecological Economics, 76, 112–118. doi: https://doi.org/10.1016/j.ecolecon.2012.02.012

349. Sumner, M. (2009). Information security threats: A comparative analysis of impact, probability, and preparedness. Information Systems Management, 26(1), 2–12. doi: https://doi.org/10.1080/10580530802384639

350. Škrinjarić, B. (2019). Internet literacy in an online environment: Influence of internet skills on internet privacy. In O. Filiposki, D. Metodijeski, & D. Zlatovic (Eds.), Proceedings of

the Fourth International Conference The Challenges of Today (pp. 165–178).

351. Škrinjarić, B. (2023). Internet skills and range of activities: Influence of internet literacy on resilience to online privacy violation. In D. Tipurić & M. Marić (Eds.), Economic and social development (Book of proceedings), 94th International Scientific Conference on Economic and Social Development "The Dark Side of Management and Governance: Power, Ideology, Tensions, and Destructive Traits" (XI. OFEL) (pp. 21–34). Retrieved from: https://www.esd-conference.com/upload/book_of_proceedings/Book_of_Proceedings_esdOFEL2023_Online.pdf

352. Škrinjarić, B., Budak, J., & Rajh, E. (2019). Perceived quality of privacy protection regulations and online privacy concern. Economic Research-Ekonomska Istraživanja, 32(1), 982–1000. doi: https://doi.org/10.1080/1331677X.2019.1585272

353. Škrinjarić, B., Budak, J., & Rajh, E. (2021). Psychometric characteristics of self-efficacy and optimism and pessimism measurement scales in online privacy violation context. International Journal of Multidisciplinarity in Business and Science, 7(12), 5–14.

354. Škrinjarić, B., Budak, J., & Rajh, E. (2022). Consumers' attitudes change in response to privacy violation online incident. Proceedings of FEB Zagreb 13th International Odyssey Conference, Dubrovnik 1.-4.6.2022. Zagreb: University of Zagreb Faculty of Economics & Business, 4(1), 391-404. doi: https://doi.org/10.22598/odyssey/2022.4

355. Škrinjarić, B., Budak, J., & Žokalj, M. (2018). The effect of personality traits on online privacy concern. Ekonomski pregled, 69(2), 106–130. doi: https://doi.org/10.32910/ep.69.2.2

356. Terlizzi, A. (2021). The digitalization of the public sector: A systematic literature review. Rivista Italiana di Politiche Pubbliche, 16(1), 5–38.

357. Thoma, K., Scharte, B., Hiller, D., & Leismann, T. (2016). Resilience engineering as part of security research: Definitions, concepts and science approaches. European Journal for Security Research, 1(1), 3–19. doi: https://doi.org/10.1007/s41125-016-0002-4

358. Thomas, J. (1994). Factors affecting computer anxiety and its effects on ease of use of business software. In M. Khosrowpour (Ed.), Managing social and economic change with information technology: Proceedings of the Information Resources Management Association International Conference (pp. 51–52). London: IDEA Group Publishing.

359. Tilman, D., & Downing, J. A. (1994). Biodiversity and stability in grasslands. Nature,

367, 363–365. doi: https://doi.org/10.1038/367363a0

360. Tran, T., Ho, M. T., Pham, T. H., Nguyen, M. H., Nguyen, K. L. P., Vuong, T. T., … Vuong, Q. H. (2020). How digital natives learn and thrive in the digital age: Evidence from an emerging economy. Sustainability, 12(9), 3819. doi: https://doi.org/10.3390/su12093819

361. Trittin-Ulbrich, H., Scherer, A. G., Munro, I., & Whelan, G. (2021). Exploring the dark and unexpected sides of digitalization: Toward a critical agenda. Organization, 28(1), 8–25. doi: https://doi.org/10.1177/1350508420968184

362. Trivedi, K. S., Kim, D. S., & Ghosh, R. (2009). Resilience in computer systems and networks. Proceedings of the 2009 International Conference on Computer-Aided Design, 74–77. ACM. doi: http://dx.doi.org/10.1145/1687399.1687415

363. Tsiakis, T. (2012). Consumers' issues and concerns of perceived risk of information security in online framework. The marketing strategies. Procedia - Social and Behavioral Sciences, 62, 1265–1270. doi: https://doi.org/10.1016/j.sbspro.2012.09.216

364. Tu, H., Doupe, A., Zhao, Z., & Ahn, G.-J. (2016). SoK: Everyone hates robocalls: A survey of techniques against telephone spam. 2016 IEEE Symposium on Security and Privacy (SP), 320–338. doi: https://doi.org/10.1109/SP.2016.27

365. Tugade, M. M., & Fredrickson, B. L. (2004). Resilient individuals use positive emotions to bounce back from negative emotional experiences. Journal of Personality and Social Psychology, 86(2), 320–333. doi: https://doi.org/10.1037/0022-3514.86.2.320

366. Tupes, E. C., & Christal, R. E. (1992). Recurrent personality factors based on trait ratings. Journal of Personality, 60(2), 225–251. doi: https://doi.org/10.1111/j.1467-6494.1992.tb00973.x

367. Ungar, M. (2008). Resilience across cultures. The British Journal of Social Work, 38(2), 218–235. doi: https://doi.org/10.1093/bjsw/bcl343

368. Ungar, M. (2011). The social ecology of resilience: Addressing contextual and cultural ambiguity of a nascent construct. American Journal of Orthopsychiatry, 81(1), 1–17. doi: https://doi.org/10.1111/j.1939-0025.2010.01067.x

369. Ungar, M., & Liebenberg, L. (2011). Assessing resilience across cultures using mixed methods: Construction of the child and youth resilience measure. Journal of Mixed Methods Research, 5(2), 126–149. Doi: https://doi.org/10.1177/1558689811400607

370. Ur, B., & Wang, Y. (2013). A cross-cultural framework for protecting user privacy in online social media. Proceedings of the 22nd International Conference on World Wide Web, 755–762. Doi: https://doi.org/10.1145/2487788.2488037

371. Vagias, W. M. (2006). Likert-type scale response anchors. Clemson International Institute for Tourism & Research Development, Department of Parks, Recreation and Tourism Management, Clemson University.

372. Valarezo, Á., López, R., & Pérez Amaral, T. (2020). Adoption of e-commerce by individuals and digital-divide. In J. Alleman, P. Rappoport, & M. Hamoudia (Eds.), Applied economics in the digital era (pp. 103–134). Cham: Palgrave Macmillan. Doi: https://doi.org/10.1007/978-3-030-40601-1_4

373. Van Heck, G. L. (1998). Personality and physical health: toward an ecological approach to health-related personality research. European Journal of Personality, 11(5), 415-443. doi: https://doi.org/10.1002/(SICI)1099-0984(199712)11:5<415::AID-PER306>3.0.CO;2-G

374. van Schaik, P., Jansen, J., Onibokun, J., Camp, J., & Kusev, P. (2018). Security and privacy in online social networking: Risk perceptions and precautionary behavior. Computers in Human Behavior, 78, 283–297. Doi: https://doi.org/10.1016/j.chb.2017.10.007

375. Van Vliet, K. J. (2008). Shame and resilience in adulthood: A grounded theory study. Journal of Counseling Psychology, 55(2), 233–245. Doi: https://doi.org/10.1037/0022-0167.55.2.233

376. van Zoonen, L. (2016). Privacy concerns in smart cities. Government Information Quarterly, 33(3), 472–480. Doi: https://doi.org/10.1016/j.giq.2016.06.004.

377. Vanderbilt-Adriance, E., & Shaw, D. S. (2008). Conceptualizing and re-evaluating resilience across levels of risk, time, and domains of competence. Clinical Child and Family Psychology Review, 11, 30–58. Doi: https://doi.org/10.1007/s10567-008-0031-2

378. Vandoninck, S., d'Haenens, L., & Roe, K. (2013). Online risks: Coping strategies of less resilient children and teenagers across Europe. Journal of Children and Media, 7(1), 60–78. Doi: https://doi.org/10.1080/17482798.2012.739780

379. Veiga, A. D., & Eloff, J. H. (2007). An information security governance framework. Information Systems Management, 24(4), 361–372. Doi: https://doi.org/10.1080/10580530701586136

380. Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. Management Science, 46(2), 186–204. Doi: https://doi.org/10.1287/mnsc.46.2.186.11926

381. Visser, W. A. (2007). Daily hassles, resilience and burnout of call centre staff. (Unpublished doctoral dissertation). North-West University, Potchefstroom.

382. Volkova, N., Kuzmuk, I., Oliinyk, N., Klymenko, I., & Dankanych, A. (2021). Development trends of the digital economy: E-business, e-commerce. International Journal of Computer Science & Network Security, 21(4), 186–198.

383. von Solms, S. B. (2005). Information security governance – Compliance management vs operational management. Computers & Security, 24(6), 443–447. Doi: https://doi.org/10.1016/j.cose.2005.07.003

384. Wagnild, G. M., & Young, H. M. (1993). Development and psychometric evaluation of the resilience scale. Journal of Nursing Measurement, 1(2), 165–178.

385. Walker, B., Carpenter, S., Anderies, J., Abel, N., Cumming, G., Janssen, M., ... Pritchard, R. (2002). Resilience management in social-ecological systems: A working hypothesis for a participatory approach. Conservation Ecology, 6(1), 14. Doi: https://doi.org/10.5751/ES-00356-060114

386. Walker, B. H., Anderies, J. M., Kinzig, A. P., & Ryan, P. (2006). Exploring resilience in social-ecological systems through comparative studies and theory development: introduction to the special issue. Ecology and society, 11(1). Retrieved from: https://www.jstor.org/stable/26267774

387. Walker, B., Holling, C. S., Carpenter, S. R., & Kinzig, A. (2004). Resilience, adaptability and transformability in social–ecological systems. Ecology and Society, 9(2), 5. Doi: https://doi.org/10.5751/ES-00650-090205

388. Walker, J., & Cooper, M. (2011). Genealogies of resilience: From systems ecology to the political economy of crisis adaptation. Security Dialogue, 42(2), 143–160. Doi: https://doi.org/10.1177/0967010611399616

389. Waller, M. (2001). Resilience in ecosystemic context: Evolution of the concept. American Journal of Orthopsychiatry, 71(3), 290–297. Doi: https://doi.org/10.1037/0002-9432.71.3.290

390. Walther, J. B. (2011). Introduction to privacy online. In S. Trepte & L. Reinecke (Eds.), Privacy online: Perspectives on privacy and self-disclosure in the social web (pp. 3–7). Berlin: Springer. doi: https://doi.org/10.1007/978-3-642-21521-6_1

391. Wang, H., Lee, M. K. O., & Wang, C. (1998). Consumer privacy concerns about internet marketing. Communications of the ACM, 41(3), 63–70. Doi: https://doi.org/10.1145/272287.272299

392. Wang, Q., Dacko, S., & Gad, M. (2008). Factors influencing consumers' evaluation and adoption intention of really-new products or services: Prior knowledge, innovativeness and timing of product evaluation. In A. Y. Lee & D. Soman (Eds.), NA – Advances in Consumer Research, Volume 35 (pp. 416–422). Duluth, MN: Association for Consumer Research. Retrieved from: http://www.acrwebsite.org/volumes/13522/volumes/v35/NA-35

393. Wang, Y. D., & Emurian, H. H. (2005). An overview of online trust: Concepts, elements, and implications. Computers in Human Behaviour, 21(1), 105–125. Doi: https://doi.org/10.1016/j.chb.2003.11.008

394. Werner, E., & Smith, R. (1992). Overcoming the odds: High risk children from birth to adulthood. Ithaca, NY: Cornell University Press. doi: https://doi.org/10.7591/9781501711992

395. Westin, A. F. (1970). Privacy and freedom [1st ed. 1967]. New York, NY: Atheneum.

396. Whitman, M. (2003). Enemy at the gate: Threats to information security. Communications of the ACM, 46(8), 91–95. Doi: https://doi.org/10.1145/859670.859675

397. Whitman, M. E., & Mattord, H. J. (2011). Principles of information security. Cengage Learning.

398. Wiktor, J. W., Dado, J., & Simberova, I. (2021). The digital transformation of the EU market: The digital single market strategy in the context of e-commerce development diversification in Czechia, Poland and Slovakia. Problemy Zarzadzania, 19(1), 11–28.

399. Wildavsky, A. (1988). Searching for safety. New Brunswick, NJ: Transaction Publishers.

400. Windle, G. (2011). What is resilience? A review and concept analysis. Reviews in Clinical Gerontology, 21(2), 152–169. Doi: https://doi.org/10.1017/S0959259810000420

401. Windle, G., Bennett, K. M., & Noyes, J. (2011). A methodological review of resilience measurement scales. Health and Quality of Life Outcomes, 9, 8. Doi: https://doi.org/10.1186/1477-7525-9-8

402. Wirtz, J., Lwin, M., & Williams, J. (2007). Causes and consequences of consumer online privacy concern. International Journal of Service Industry Management, 18(4), 326–348. Doi: https://doi.org/10.1108/09564230710778128

403. Wolfond, G. (2017). A blockchain ecosystem for digital identity: Improving service delivery in Canada's public and private sectors. Technology Innovation Management Review, 7(10), 35–40. Doi: https://doi.org/10.22215/timreview/1112

404. Woods, D. D. (2017). Essential characteristics of resilience. In D. D. Woods (Ed.), Resilience engineering (pp. 21–34). CRC Press. doi: https://doi.org/10.1201/9781315605685-4

405. Xu, H., Dinev, T., Smith, H. J., & Hart, P. (2008). Examining the formation of individual's privacy concerns: Toward an integrative view. Proceedings of the 29th International Conference on Information Systems, 1–16. Paris: Association for Information Systems Electronic Library (AISeL).

406. Xu, H., Luo, X. R., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. Decision Support Systems, 51(1), 42–52. Doi: https://doi.org/10.1016/j.dss.2010.11.017

407. Yao, M. Z. (2011). Self-protection of online privacy: A behavioral approach. In S. Trepte & L. Reinecke (Eds.), Privacy online: Perspectives on privacy and self-disclosure in the social web (pp. 111–125). Berlin: Springer. doi: https://doi.org/10.1007/978-3-642-21521-6_9

408. Yao, M. Z., Rice, R. E., & Wallis, K. (2007). Predicting user concerns about online privacy. Journal of the American Society for Information Science and Technology, 58, 710–722. doi: https://doi.org/10.1002/asi.20530

409. Yoo, B., Donthu, N., & Lee, S. (2000). An examination of selected marketing mix elements and brand equity. Journal of the Academy of Marketing Science, 28(2), 195–211. doi: https://doi.org/10.1177/0092070300282002

410. Yoon, C. (2011). Theory of planned behavior and ethics theory in digital piracy: An integrated model. Journal of Business Ethics, 100, 405–417. doi: https://doi.org/10.1007/s10551-010-0687-7

411. Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. IEEE Internet of Things Journal, 1(1), 22–32. doi: https://doi.org/10.1109/JIOT.2014.2306328

412. Zautra, A. J., Johnson, L. M., & Davis, M. C. (2005). Positive affect as a source of resilience for women in chronic pain. Journal of Consulting and Clinical Psychology, 73(2), 212–220. doi: https://doi.org/10.1037/0022-006X.73.2.212

413. Zhang, R., Chen, J. Q., & Lee, C. J. (2013). Mobile commerce and consumer privacy concerns. Journal of Computer Information Systems, 53(4), 31–38. doi: https://doi.org/10.1080/08874417.2013.11645648

414. Ziesak, J. (2013). The dark side of personalization: Online privacy concerns influence customer behavior. Hamburg: Anchor Academic Publishing.

415. Zukowski, T., & Brown, I. (2007). Examining the influence of demographic factors on internet users' information privacy concerns. Proceedings of the 2007 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries, 197–204. doi: https://doi.org/10.1145/1292491.1292514

416. Zureik, E. (2004). Globalization of Personal Data project – international survey concept paper. In The Surveillance Project Public Opinion Workshop, 3 March 2004, Kingston, ON.

Appendix 1. Types and definitions of resilience

Type of resilience	Definition of resilience	Reference
Physical resilience	The ability to store strain energy and deflect elastically under a load without breaking or being deformed.	Gordon (1978)
	The speed with which a system returns to equilibrium after displacement, irrespective of how many oscillations are required.	Bodin and Wiman (2004)
Ecological and ecosystems resilience	Measure of the persistence of systems and of their ability to absorb change and disturbance and still maintain the same relationships between populations or state variables. The persistence of relationships within a system; a measure of the ability of systems to absorb changes of state variables, driving variables, and parameters, and still persist.	Holling (1973)
	The ability to maintain the functionality of a system when it is perturbed or the ability to maintain the elements required to renew or reorganize if a disturbance alters the structure or function of a system.	Walker et al. (2002)
	The capacity of a system to absorb a disturbance and reorganize while undergoing change while retaining the same function, structure, identity, and feedback.	Walker et al. (2004)
	The magnitude of disturbance that a system can absorb before its structure is redefined by changing the variables and processes that control behavior.	Gunderson (2000)
	The speed at which a system returns to a single equilibrium point following a disruption.	Tilman and Downing (1994)
	Positive adaptation in response to adversity; it is not the absence of vulnerability, not an inherent characteristic, and not static.	Waller (2001)
	Quantitative property that changes throughout ecosystem dynamics and occurs on each level of an eco-system's hierarchy.	Holling (2001)
	The underlying capacity of an ecosystem to maintain desired ecosystem services in the face of a fluctuating environment and human use.	Folke et al. (2002)
	The magnitude of disturbance that can be absorbed before the system changes its structure by changing the variables and processes that control behavior.	Gunderson and Holling (2002)
	The ability of a system that has undergone stress to recover and return to its original state; more precisely: (i) the amount of disturbance a system can absorb and still remain within the same state or domain of attraction; and (ii) the degree to which the system is capable of self-organization.	Klein et al. (2003)
	The capacity of a social-ecological system to absorb recurrent disturbances (...) so as to retain essential structures, processes, and feedbacks.	Adger et al. (2005)
Sociological and community resilience	The ability of an individual, group, or organization to continue its existence (or remain more or less stable) in the face of some sort of surprise. Resilience is found in systems that are highly adaptable (not locked into specific strategies) and have diverse resources.	Longstaff (2005)
	The ability of groups or communities to withstand external shocks to their social infrastructure.	Adger (2000)
	The capacity of a system to experience shocks while retaining essentially the same function, structure, feedbacks, and therefore identity.	Walker et al. (2006)
	The ability of social units to mitigate hazards, contain the effects of disasters when they occur, and carry out recovery activities in ways that minimize social disruption and mitigate the effects of future earthquakes.	Bruneau et al. (2003)
	The ability to recover from or adjust easily to misfortune or sustained life stress.	Brown and Perkins (1992)
	The process through which mediating structures (schools, peer groups, family) and activity settings moderate the impact of oppressive systems.	Sonn and Fisher (1998)
	The capability to bounce back and to use physical and economic resources effectively to aid recovery following exposure to hazards.	Paton, Millar, and Johnston (2000)
	The ability of individuals and communities to deal with a state of continuous, long-term stress; the ability to find unknown inner strengths and resources in order to cope effectively; the measure of adaptation and flexibility.	Ganor and Ben-Lavy (2003)
	The development of material, physical, socio-political, socio-cultural, and psychological resources that promote safety of residents and buffer adversity.	Ahmed et al. (2004)

Type of resilience	Definition of resilience	Reference
Sociological and community resilience	Individuals' sense of the ability of their own community to deal successfully with ongoing political violence.	Kimhi and Shamai (2004)
	A community's capacities, skills, and knowledge that allow it to participate fully in recovery from disasters.	Coles and Buckle (2004)
	The ability of community members to take meaningful, deliberate, collective action to remedy the impact of a problem, including the ability to interpret the environment, intervene, and move on.	Pfefferbaum et al. (2005)
	The magnitude of disturbance that a system can tolerate before it transitions into a different state that is controlled by a different set of processes.	Carpenter et al. (2001)
Psychology and individual resilience	The process of, capacity for, or outcome of successful adaptation despite challenging or threatening circumstances.	Masten et al. (1990)
	The capacity for successful adaptation, positive functioning, or competence (...) despite high-risk status, chronic stress, or following prolonged or severe trauma.	Egeland, Carlson, and Sroufe (1993)
	Good adaptation under extenuating circumstances; a recovery trajectory that returns to baseline functioning following a challenge.	Butler, Morland, and Leskin (2007)
	Resilient individuals possess three common characteristics. These include an acceptance of reality, a strong belief that life is meaningful, and the ability to improvise.	Coutu (2002)
	The developable capacity to rebound from adversity.	Luthans et al. (2006)
	Protective factors which modify, ameliorate, or alter a person's response to some environmental hazard that predisposes to a maladaptive outcome.	Rutter (1987)
	A dynamic process encompassing positive adaptation within the context of significant adversity.	Luthar et al. (2000)
	A class of phenomena characterized by good outcomes in spite of serious threats to adaptation or development.	Masten (2001)
	The personal qualities that enable one to thrive in the face of adversity.	Connor and Davidson (2003)
	The ability of adults in otherwise normal circumstances, who are exposed to an isolated and potentially highly disruptive event such as the death of a close relation or a violent or life-threatening situation, to maintain relatively stable, healthy levels of psychological and physical functioning, as well as the capacity for generative experiences and positive emotions.	Bonanno (2004)
	The capacity of individuals to cope successfully with significant change, adversity, or risk.	Lee and Cranford (2008)
	Complex repertoire of behavioral tendencies.	Agaibi and Wilson (2005)
	An individual's stability or quick recovery (or even growth) under significant adverse conditions.	Leipold and Greve (2009)
Disaster management	The ability of social units to mitigate hazards, contain the effects of disasters when they occur, and carry out recovery activities that minimize social disruption and mitigate the effects of future earthquakes.	Bruneau et al. (2003)
	Resilience describes an active process of self-righting, learned resourcefulness, and growth. The concept relates to the ability to function at a higher psychological level, given an individual's capabilities and previous experience.	Paton, Smith, and Violanti (2000)
Economic	The ability of a system to withstand either market or environmental shocks without losing the capacity to allocate resources efficiently.	Perrings (2006)
City	A sustainable network of physical systems and human communities, capable of managing extreme events; during disaster, both must be able to survive and function under extreme stress.	Godschalk (2003)
Engineering	The ability to sense, recognize, adapt, and absorb variations, changes, disturbances, disruptions, and surprises.	Hollnagel, Woods, and Leveson (2006)

Appendix 2. Questionnaire in Croatian (original)

Poštovani,

Ekonomski institut, Zagreb provodi istraživanje o narušavanju Vaše privatnosti u online okruženju, npr. na internetu. Narušavanje privatnosti online je neovlašteno prikupljanje, korištenje i dijeljenje osobnih informacija Vas kao korisnika interneta bez Vašeg dopuštenja.

Cijenimo Vaše sudjelovanje u našem istraživanju. Napominjemo da je anketa potpuno anonimna, a Vaši će odgovori biti predstavljeni samo u zbirnom obliku (npr. u tablicama s postocima).

1. (F1) Koristite li se internetom na bilo kojem uređaju? (npr. računalu, laptopu, tabletu, pametnom telefonu i slično)

1 – Da	2 – Ne	(ako NE, kraj)

2. (F2) Prema Vašoj subjektivnoj procjeni, jeste li doživjeli narušavanje privatnosti na internetu u posljednje tri godine? (Pod povredom privatnosti smatramo bilo koji slučaj gdje ste Vi osjetili da Vam je online privatnost narušena, npr.: i) slučaj kad internetske tražilice neovlašteno snimaju Vaše aktivnosti na internetu; ii) neovlašteno prepoznavanje lokacije gdje se krećete putem pametnog telefona; iii) neovlašteno slanje personaliziranih reklama koje su omogućili "kolačići" na web stranici; iv) neovlašten "upad" u Vaš račun elektroničke pošte; v) neovlašteno korištenje osobnih podataka koje stavljate na društvene mreže; vi) krađa lozinke, PIN-a ili broja kreditne kartice; vii) slično)

1 – Da	2 – Ne	(ako NE, kraj)

3. (PV1) Ukratko opišite zadnji incident narušavanja Vaše privatnosti online.
[otvoreno pitanje]

4. (PV2) Koliko je ozbiljan bio taj slučaj povrede privatnosti online za Vas?

1 – Zanemarivo ozbiljan	2 – Umjereno ozbiljan	3 – Osrednje ozbiljan	4 – Ozbiljan	5 – Veoma ozbiljan

5. (RES) Navedite u kojoj se mjeri slažete sa svakom od sljedećih izjava.

1 – Uopće se ne slažem	2 – Ne slažem se	3 – Neutralan	4 – Slažem se	5 – U potpunosti se slažem

res_1 Brzo sam zaboravio/zaboravila posljednji slučaj narušavanja privatnosti online.	1	2	3	4	5
res_2 Teško sam se nosio/nosila s posljednjim slučajem narušavanja privatnosti online.	1	2	3	4	5
res_3 Nije trebalo dugo da se oporavim od posljednjeg slučaja narušavanja privatnosti online.	1	2	3	4	5
res_4 Bilo mi je teško vratiti se na staro nakon posljednjeg slučaja narušavanja privatnosti online.	1	2	3	4	5
res_5 Prebrodio/prebrodila sam posljednji slučaj narušavanja privatnosti online bez previše problema.	1	2	3	4	5
res_6 Trebalo mi je puno vremena da taj događaj ostavim “iza sebe”.	1	2	3	4	5

6. (ATT) Opišite kako su se Vaše ponašanje i stav promijenili nakon narušavanja privatnosti na internetu.

(att_1) Nakon incidenta s narušavanjem privatnosti na internetu, koristim internet:

1 – Mnogo rjeđe	2 – Rjeđe	3 – Jednako kao i prije	4 – Češće	5 – Puno češće

(att_2) Nakon incidenta s narušavanjem privatnosti na internetu, moja razina opreznosti kada sam na internetu je:

1 – Puno manja	2 – Manja	3 – Jednako kao i prije	4 – Viša	5 – Puno viša

(att_3) Nakon incidenta s narušavanjem privatnosti na internetu, raspon aktivnosti koje obavljam putem interneta:

1 – Dramatično se smanjio	2 – Smanjio se	3 – Ostao je isti	4 – Povećao se	5 – Dramatično se povećao

(att_4) Nakon incidenta s narušavanjem privatnosti na internetu, moj stav prema internetu je postao:

1 – Puno negativniji	2 – Negativniji	3 – Nepromijenjen	4 – Pozitivniji	5 – Puno pozitivniji

7. (T) Procijenite koliko vremena u uobičajenom danu aktivno provedete na internetu (u satima)?

(t_1) _____ sati za PRIVATNE razloge	(t_2) _____ sati za POSLOVNE razloge

8. (WEB) Koliko često obavljate sljedeće aktivnosti na internetu?

1 – Nikada	2 – Rijetko	3 – Ponekad	4 – Često	5 – Vrlo često

web_1 Primanje i slanje e-mailova	1	2	3	4	5
web_2 Korištenje chat/instant message servisa (npr. WhatsApp, Viber, Messenger)	1	2	3	4	5
web_3 Preuzimanje (download) glazbe i/ili filmova	1	2	3	4	5
web_4 Igranje online igrica	1	2	3	4	5
web_5 Plaćanje računa/korištenje internetskog bankarstva	1	2	3	4	5
web_6 Pohađanje nastave, kolegija ili tečaja online	1	2	3	4	5
web_7 Kupovina putem interneta	1	2	3	4	5
web_8 Live streaming i/ili gledanje multimedijskih sadržaja (npr. YouTube, online radio)	1	2	3	4	5
web_9 Korištenje audio/video poziva i/ili sastanaka (npr. Skype, Zoom)	1	2	3	4	5
web_10 Korištenje društvenih mreža (npr. Facebook, Twitter, Instagram, TikTok)	1	2	3	4	5
web_11 Praćenje dnevnih vijesti	1	2	3	4	5
web_12 Korištenje pretraživača za opće informacije (npr. Google)	1	2	3	4	5
web_13 Traženje karte i uputa za vožnju	1	2	3	4	5
web_14 Aktivno sudjelovanje na online forumima	1	2	3	4	5
web_15 Korištenje online servisa javne uprave (npr. e-građani, online prijava poreza, e-upisi, e-dnevnik, postani student)	1	2	3	4	5

9. (EBUY) Jeste li ikada kupili proizvod ili uslugu putem interneta?

1 – DA	2 – NE

10. (SKILL) Koliko ste sposobni obavljati sljedeće radnje povezane s internetom?

1 – Uopće ne	2 – Ne tako dobro	3 – Relativno dobro	4 – Dobro	5 – Izrazito dobro

skill_1 Mogu koristiti internetski preglednik (npr. Chrome, Firefox, Safari) za surfanje internetom.	1	2	3	4	5
skill_2 Mogu otvoriti novu adresu e-pošte (npr. Gmail) ili društvene mreže (npr. Facebook).	1	2	3	4	5
skill_3 Mogu uređivati označene stranice (bookmarks).	1	2	3	4	5
skill_4 Mogu spremiti sadržaj s internetske stranice na disk.	1	2	3	4	5
skill_5 Mogu administrirati internetsku stranicu.	1	2	3	4	5
skill_6 Mogu kreirati internetsku stranicu.	1	2	3	4	5

11. U kojoj mjeri se slažete sa sljedećim tvrdnjama?

1 – Uopće se ne slažem	2 – Ne slažem se	3 – Neutralan	4 – Slažem se	5 – U potpunosti se slažem

pt_1 Smatram se rezerviranom osobom.	1	2	3	4	5
pt_2 Smatram se osobom koja ima povjerenja u druge ljude.	1	2	3	4	5
pt_3 Smatram se lijenom osobom.	1	2	3	4	5
pt_4 Smatram se opuštenom osobom koja dobro podnosi stres.	1	2	3	4	5
pt_5 Smatram se osobom zainteresiranom za umjetnost.	1	2	3	4	5
pt_6 Smatram se društvenom osobom.	1	2	3	4	5
pt_7 Smatram se osobom koja prebacuje krivnju na druge.	1	2	3	4	5
pt_8 Smatram se temeljitom osobom.	1	2	3	4	5
pt_9 Smatram se nervoznom osobom.	1	2	3	4	5
pt_10 Smatram se osobom bujne mašte.	1	2	3	4	5
opt_1 Stvari uvijek gledam s vedrije strane.	1	2	3	4	5
opt_2 Uvijek sam optimističan glede svoje budućnosti.	1	2	3	4	5
opt_3 Općenito gledajući, stvari uvijek ispadnu dobro.	1	2	3	4	5
pes_1 Rijetko očekujem da će se dogoditi nešto dobro.	1	2	3	4	5
pes_2 Stvari se nikad ne odvijaju kako želim.	1	2	3	4	5
pes_3 Bolje je očekivati neuspjeh jer Vas tada manje potrese kad se zaista dogodi.	1	2	3	4	5
se_1 Imam visoko samopouzdanje.	1	2	3	4	5
sef_1 Lako mi je držati se svojih ciljeva i ostvariti ih.	1	2	3	4	5
sef_2 Zahvaljujući svojoj snalažljivosti, znam kako se treba nositi s nepredvidivim situacijama.	1	2	3	4	5
sef_3 Mogu riješiti većinu problema ako uložim dovoljno truda.	1	2	3	4	5
sef_4 Kada se suočavam s teškoćama, mogu ostati pribran jer se oslanjam na svoje sposobnosti suočavanja.	1	2	3	4	5
oaw_1 Upoznat sam s pitanjima privatnosti i rješenjima koje poduzeća i vlada uvode kako bi osigurali našu online privatnost.	1	2	3	4	5
oaw_2 Web stranice koje zahtijevaju informacije o meni trebaju objaviti način na koji se podaci prikupljaju, obrađuju i koriste.	1	2	3	4	5
oaw_3 Kvalitetna politika zaštite online privatnosti treba biti jasno vidljiva.	1	2	3	4	5

st_1 Općenito, imam povjerenja u ljude.	1	2	3	4	5
st_2 Općenito, imam povjerenja u javne institucije na razini države.	1	2	3	4	5
st_3 Općenito, imam povjerenja u lokalne javne institucije.	1	2	3	4	5
st_4 Općenito, imam povjerenja u svoju lokalnu zajednicu (npr. susjedstvo, ljudi koji me okružuju).	1	2	3	4	5
gias_1 Općenito, imam pozitivan stav prema internetu.	1	2	3	4	5
bnf_1 Općenito, moja potreba za dobivanjem određenih informacija ili usluga s interneta je veća od moje zabrinutosti za online privatnost.	1	2	3	4	5
bnf_2 Što su moji interesi za dobivanje informacija ili usluga s interneta veći, to sam manje zabrinut za svoju online privatnost.	1	2	3	4	5
da_1 Digitalizacija je ozbiljna prijetnja privatnosti.	1	2	3	4	5
da_2 Zabrinut sam zbog tempa razvoja digitalizacije u mom životu.	1	2	3	4	5
dps_1 Pod pretpostavkom da imam pristup digitalnim javnim uslugama, namjeravam ih koristiti. (Za anketare: npr. e-građani, online prijava poreza, e-upisi, ...)	1	2	3	4	5
dps_2 Kada bih imao pristup digitalnim javnim uslugama, mislim da bih ih koristio. (Za anketare: npr. e-građani, online prijava poreza, e-upisi, ...)	1	2	3	4	5
ldps_1 Pod pretpostavkom da imam pristup digitalnim javnim uslugama u mom gradu ili općini, namjeravam ih koristiti (npr. sustav pametnog parkiranja, web kamere, besplatni WiFi na odabranim lokacijama u općini ili gradu, odvoz otpada, elektroničke karte u javnom prijevozu…).	1	2	3	4	5
ldps_2 Kada bih imao pristup digitalnim javnim uslugama u mom gradu ili općini, mislim da bih ih koristio (npr. sustav pametnog parkiranja, web kamere, besplatni WiFi na odabranim lokacijama u općini ili gradu, odvoz otpada, elektroničke karte u javnom prijevozu…).	1	2	3	4	5
opc_1 Zabrinut sam za moju privatnost u online okruženju.	1	2	3	4	5
opc_2 Brine me pretjerano prikupljanje mojih osobnih informacija na internetu.	1	2	3	4	5
opc_3 Brine me narušavanje moje privatnosti kada se služim internetom.	1	2	3	4	5
reg_1 Postojeći zakoni u Hrvatskoj su dovoljni da se zaštiti privatnost građana na internetu.	1	2	3	4	5
reg_2 Vlada u mojoj zemlji čini dovoljno da zaštiti građane od narušavanja online privatnosti.	1	2	3	4	5
sh_1 Prihvatljivo mi je javno podijeliti privatne informacije na internetu.	1	2	3	4	5
sh_2 Prihvatljivo mi je na internetu javno objaviti gdje se trenutno nalazim.	1	2	3	4	5
sh_3 Prihvatljivo mi je na internetu javno objaviti s kime trenutno provodim vrijeme.	1	2	3	4	5
sh_4 Prihvatljivo mi je poslati podatke s moje kreditne kartice kad kupujem online.	1	2	3	4	5

12. (PB) Koliko često obavljate sljedeće aktivnosti na internetu?

1 – Nikada	2 – Rijetko	3 – Ponekad	4 – Često	5 – Vrlo često

pb_1 Dajem pogrešne odgovore kako bih izbjegao odavanje pravih informacija o sebi.	1	2	3	4	5
pb_2 Koristim drugo ime ili e-mail adresu pri registraciji na web stranici bez otkrivanja svojeg pravog identiteta.	1	2	3	4	5
pb_3 Prilikom registracije na neku web stranicu, ako je to moguće, podatke ispunjavam samo djelomično.	1	2	3	4	5
pb_4 Pokušavam eliminirati kolačiće (cookies) koji prate moje aktivnosti na internetu.	1	2	3	4	5
pb_5 Pokušavam prikriti svoj identitet prilikom surfanja na internetu (opcija privatnog surfanja).	1	2	3	4	5
pb_6 Odbijam otkriti osobne informacije nepouzdanim web stranicama.	1	2	3	4	5

13. (SS1) Koliko lako možete dobiti praktičnu pomoć vezanu uz korištenje interneta od ljudi koji su Vam bliski (članova Vaše obitelji, prijatelja, kolega...) ako bi Vam trebala?

1 – Veoma teško	2 – Teško	3 – Moguće je	4 – Lako	5 – Veoma lako

14. (IT1) Koliko ste zainteresirani za korištenje novih online usluga ili tehnologija neposredno po njihovom uvođenju?

1 – U potpunosti nezainteresiran	2 – Nezainteresiran	3 – Neutralan	4 – Zainteresiran	5 – U potpunosti zainteresiran

15. (D1) Spol

M	Ž

16. (D2) Dob:

17. (D3) Najviši završeni stupanj obrazovanja:

1 – Osnovna škola ili manje	2 – Srednja škola	3 – Viša škola ili fakultet	4 – Poslijediplomski studij (doktorat, poslijediplomski specijalistički studij, MBA, …)

18. (D4) Broj članova Vašeg kućanstva?

19. (D5) Vaše zanimanje?

1 – Vlasnik poduzeća ili obrta	2 – Rukovoditelj (manager)	3 – Stručnjak (VSS ili više, npr. liječnik, odvjetnik, računovođa, inženjer)	4 – Službenik (radi uglavnom u uredu)
5 – Radnik	6 – Umirovljenik	7 – Student	8 – Nezaposlen
9 – Neko drugo zanimanje, koje?			

20. (D6) Ukupna mjesečna primanja Vašeg kućanstva?

1 – Do 2.500 kn	2 – 2.501–3.500 kn	3 – 3.501–5.000 kn	4 – 5.001–6.500 kn	5 – 6.501–8.000 kn	6 – 8.001–10.000 kn
7 – 10.001–12.000 kn	8 – 12.001–15.000 kn	9 – 15.001–20.000 kn	10 – Više od 20.000 kn	11 – Ne želim odgovoriti	

21. (D7) Županija:

22. (D8) Grad/općina:

23. (D9) Veličina Vašeg mjesta prema broju stanovnika?

1 – 10.000 ili manje	2 – 10.001–50.000	3 – 50.001–100.000	4 – Više od 100.000

Anketar:

Datum:

Sat/minute:

Broj telefona i/ili e-pošta za daljnje upite:

Appendix 3. Questionnaire in English

Dear Sir/Madam,

The Institute of Economics, Zagreb is conducting a survey-based research on privacy violation in an online environment (e.g., on the Internet). Violation of privacy on the Internet includes the unauthorized collection, disclosure, or other use of personal information without your consent.

Your participation in our research is highly appreciated. Please note that the survey is completely anonymous, and your answers will be presented in an aggregate form only (e.g., in tables with percentages).

1. (F1) Are you an Internet user? (on any device, e.g., computer, laptop, tablet, smartphone, or similar)

1 – Yes	2 – No	(if NO, stop the interview)

2. (F2) Based on your subjective perception, have you had any privacy violation issues on the Internet in the last three years? (By privacy violation issues on the Internet we consider, for example: i) instances when Internet search engines record your activities on the Internet without authorization; ii) unauthorized identification of your location via a smartphone; iii) unauthorized sending of personalized advertisements enabled by "cookies" on a website; iv) unauthorized "intrusion" into your e-mail account; v) unauthorized use of personal data posted on social networks; vi) theft of password, PIN, credit card number, or other private data; vii) any other case where you feel that your online privacy has been violated)

1 – Yes	2 – No	(if NO, stop the interview)

3. (PV1) In short, please describe the privacy violation incident. [open-ended question]

4. (PV2) How serious was this case of online privacy violation for you?

1 – Negligibly serious	2 – Somewhat serious	3 – Moderately serious	4 – Serious	5 – Very serious

5. (RES) Please indicate the extent to which you agree with each of the following statements?

1 – Strongly disagree	2 – Disagree	3 – Neutral	4 – Agree	5 – Strongly agree

res_1 I bounced back quickly after the most recent online privacy violation incident.	1	2	3	4	5
res_2 I had a hard time making it through after the most recent online privacy violation incident.	1	2	3	4	5
res_3 It didn't take me long to recover from the most recent online privacy violation incident.	1	2	3	4	5
res_4 It was hard for me to snap back when the most recent online privacy violation happened.	1	2	3	4	5
res_5 I came through the most recent online privacy violation incident with little trouble.	1	2	3	4	5
res_6 It took me a long time to get over the most recent online privacy violation incident.	1	2	3	4	5

6. (ATT) Please describe how your behavior and attitude changed after the online privacy breach.

(att_1) After the online privacy violation incident, I use the Internet:

1 – Much less frequently	2 – Less frequently	3 – The same	4 – More frequently	5 – Much more frequently

(att_2) After the online privacy violation incident, my level of cautiousness on the Internet:

1 – Dramatically decreased	2 – Slightly decreased	3 – Remained the same	4 – Slightly increased	5 – Dramatically increased

(att_3) After the online privacy violation incident, the range of activities I perform on the Internet has:

1 – Dramatically decreased	2 – Slightly decreased	3 – Remained the same	4 – Slightly increased	5 – Dramatically increased

(att_4) After the online privacy violation incident, my attitude toward the Internet became:

1 – Much more negative	2 – More negative	3 – Unchanged	4 – More positive	5 – Much more positive

7. (T) Please estimate how many hours in a typical day you spend online for private and work-related reasons?

(t_1) _____ hours for PRIVATE reasons	(t_2) _____ hours for WORK-RELATED reasons

8. (WEB) How often do you perform the following activities on the Internet?

1 – Never	2 – Rarely	3 – Sometimes	4 – Often	5 – Very often				
web_1 Receiving and sending e-mails				1	2	3	4	5
web_2 Using chat/instant message services (e.g., Messenger, WhatsApp, Viber)				1	2	3	4	5
web_3 Downloading music and/or movies				1	2	3	4	5
web_4 Playing online games				1	2	3	4	5
web_5 Paying bills/e-banking				1	2	3	4	5
web_6 Attending courses online				1	2	3	4	5
web_7 Online shopping				1	2	3	4	5
web_8 Live streaming and/or watching multimedia content (e.g., YouTube, online radio)				1	2	3	4	5
web_9 Making audio/video calls and/or meetings (e.g., Skype, Zoom)				1	2	3	4	5
web_10 Using social networks (e.g., Facebook, Twitter, Instagram, TikTok)				1	2	3	4	5
web_11 Following daily news online				1	2	3	4	5
web_12 Using search engines to find information (e.g., Google)				1	2	3	4	5
web_13 Searching for maps and driving directions				1	2	3	4	5
web_14 Using online forums				1	2	3	4	5
web_15 Using public services available online (e.g., e-građani, filing taxes online, e-upisi, e-dnevnik, postani student)				1	2	3	4	5

9. (EBUY) Have you ever bought goods or services on the Internet?

1 – YES	2 – NO

10. (SKILL) Please rate how well you can perform various Internet-related tasks.

1 – Not at all	2 – Not so well	3 – Okay	4 – Well	5 – Very well				
skill_1 I can use a browser (e.g., Chrome, Firefox, Safari) to navigate the Internet.				1	2	3	4	5
skill_2 I can register a new e-mail address (e.g., Gmail) or social network (e.g., Facebook) account.				1	2	3	4	5
skill_3 I can work with/edit bookmarks.				1	2	3	4	5
skill_4 I can save content from websites to my device.				1	2	3	4	5
skill_5 I can administer a website.				1	2	3	4	5
skill_6 I can create a website.				1	2	3	4	5

11. To what extent do you agree with the following statements?

1 – Absolutely no	2 – No	3 – Neutral	4 – Yes	5 – Absolutely yes				
pt_1 I see myself as someone who is reserved.				1	2	3	4	5
pt_2 I see myself as someone who is generally trusting.				1	2	3	4	5
pt_3 I see myself as someone who tends to be lazy.				1	2	3	4	5
pt_4 I see myself as someone who is relaxed and handles stress well.				1	2	3	4	5
pt_5 I see myself as someone who has artistic interests.				1	2	3	4	5
pt_6 I see myself as someone who is outgoing, sociable.				1	2	3	4	5
pt_7 I see myself as someone who tends to find fault with others.				1	2	3	4	5
pt_8 I see myself as someone who does a thorough job.				1	2	3	4	5
pt_9 I see myself as someone who gets nervous easily.				1	2	3	4	5
pt_10 I see myself as someone who has an active imagination.				1	2	3	4	5
opt_1 I always look on the bright side of things.				1	2	3	4	5
opt_2 I'm always optimistic about my future.				1	2	3	4	5
opt_3 In general, things turn out all right in the end.				1	2	3	4	5
pes_1 Rarely do I expect good things to happen.				1	2	3	4	5
pes_2 Things never work out the way I want them to.				1	2	3	4	5
pes_3 Better to expect defeat: then it doesn't hit so hard when it comes.				1	2	3	4	5
se_1 I have high self-esteem.				1	2	3	4	5
sef_1 It is easy for me to stick to my aims and accomplish my goals.				1	2	3	4	5
sef_2 Thanks to my resourcefulness, I know how to handle unforeseen situations.				1	2	3	4	5
sef_3 I can solve most problems if I invest the necessary effort.				1	2	3	4	5
sef_4 I can remain calm when facing difficulties because I can rely on my coping abilities.				1	2	3	4	5
oaw_1 I keep myself updated about privacy issues and the solutions that companies and the government employ to ensure our online privacy.				1	2	3	4	5
oaw_2 Websites seeking information about me should disclose the way the data are collected, processed, and used.				1	2	3	4	5
oaw_3 A good online privacy policy should have a clear and conspicuous disclosure.				1	2	3	4	5

st_1 In general, I trust people.	1	2	3	4	5
st_2 In general, I trust state public institutions.	1	2	3	4	5
st_3 In general, I trust local/municipal public institutions.	1	2	3	4	5
st_4 In general, I trust my local community (e.g., neighbors, people that surround me).	1	2	3	4	5
gias_1 In general, I have a positive attitude toward the Internet.	1	2	3	4	5
bnf_1 In general, my need to obtain certain information or services from the Internet is greater than my concern about online privacy.	1	2	3	4	5
bnf_2 The greater my interest to obtain a certain information or service from the Internet, the more I tend to suppress my online privacy concerns.	1	2	3	4	5
da_1 Digitalization is a real threat to privacy.	1	2	3	4	5
da_2 I am easily frustrated by increased digitalization in my life.	1	2	3	4	5
dps_1 Assuming I have access to digital public services, I intend to use them.	1	2	3	4	5
dps_2 If I had access to digital public services, I predict that I would use them.	1	2	3	4	5
ldps_1 Assuming I have access to digital public services in my city or municipality, I intend to use them (e.g., smart parking system, web cameras, free WiFi, waste management, e-tickets in public transport, ...).	1	2	3	4	5
ldps_2 If I had access to digital public services in my city or municipality, I predict that I would use them (e.g., smart parking system, web cameras, free WiFi, waste management, e-tickets in public transport, ...).	1	2	3	4	5
opc_1 I am concerned about my online privacy.	1	2	3	4	5
opc_2 I am concerned about extensive collection of my personal information over the Internet.	1	2	3	4	5
opc_3 I am concerned about my privacy violation when using the Internet.	1	2	3	4	5
reg_1 The existing laws in my country are sufficient to protect peoples' online privacy.	1	2	3	4	5
reg_2 The government is doing enough to ensure that citizens are protected against online privacy violations.	1	2	3	4	5
sh_1 I don't mind sharing private information publicly on the Internet.	1	2	3	4	5
sh_2 I don't mind posting my current location publicly on the Internet.	1	2	3	4	5
sh_3 I don't mind posting with whom I am at the moment publicly on the Internet.	1	2	3	4	5
sh_4 I see no problem in sending my credit card data when buying online.	1	2	3	4	5

12. (PB) How often do you perform the following activities on the Internet?

1 – Never	2 – Rarely	3 – Sometimes	4 – Often	5 – Very often

pb_1 I give fictitious responses to avoid giving websites real information about myself.	1	2	3	4	5
pb_2 I use another name or e-mail address when registering on a website without divulging my real identity.	1	2	3	4	5
pb_3 When registering on a website, if possible, I only fill in data partially.	1	2	3	4	5
pb_4 I try to eliminate cookies that track my Internet activities.	1	2	3	4	5
pb_5 I try to disguise my identity when browsing (private browsing option).	1	2	3	4	5
pb_6 I refuse to provide personal information to untrustworthy websites.	1	2	3	4	5

13. (SS1) How easy can you get practical help in using the Internet from people close to you (members of your family, friends, colleagues, …) if you should need it?

1 – Very difficult	2 – Difficult	3 – Possible	4 – Easy	5 – Very easy

14. (IT1) How interested would you be in using new online services/technologies immediately after they are available?

1 – Not interested at all	2 – Not interested	3 – Neutral	4 – Interested	5 – Very interested

15. (D1) Gender

M	F

16. (D2) Age:

17. (D3) Highest attained level of education:

1 – Primary school or less	2 – Secondary education (high school)	3 – Tertiary education (university, college)	4 – Post-graduate education (PhD, MBA, …)

18. (D4) How many people (including yourself) live in your household?

19. (D5) What is your occupation?

1 – Owner of the company/sole proprietorship own-account worker	2 – Manager/official	3 – Professional (highly educated, e.g., medical doctor, lawyer, accountant, engineer, etc.)	4 – Technician/clerk
5 – Worker	6 – Retired	7 – Student	8 – Unemployed
9 – Other, please specify:			

20. (D6) What is the net average monthly income of your household?

1 – Up to 2,500 HRK	2 – 2,501–3,500 HRK	3 – 3,501–5,000 HRK	4 – 5,001–6,500 HRK	5 – 6,501–8,000 HRK	6 – 8,001–10,000 HRK
7 – 10,001–12,000 HRK	8 – 12,001–15,000 HRK	9 – 15,001–20,000 HRK	10 – More than 20,000 HRK	11 – I do not want to answer.	

21. (D7) County:

22. (D8) Settlement:

23. (D9) Size of your settlement (number of inhabitants)?

1 – 10,000 or less	2 – 10,001–50,000	3 – 50,001–100,000	4 – More than 100,000

Interviewer:

Date:

Hour/minutes:

Phone number and/or e-mail for further inquiries:

Appendix 4. Latent variables descriptive statistics

Latent construct	Item	Description	Mean	St. dev.	Min.	Max.
Resilience to online privacy violation	res_1	I bounced back quickly after the most recent online privacy violation incident.	2.93	1.22	1	5
	res_2	I had a hard time making it through after the most recent online privacy violation incident.	2.57	1.23	1	5
	res_3	It didn't take me long to recover from the most recent online privacy violation incident.	3.32	1.21	1	5
	res_4	It was hard for me to snap back when the most recent online privacy violation happened.	2.41	1.18	1	5
	res_5	I came through the most recent online privacy violation incident with little trouble.	3.55	1.16	1	5
	res_6	It took me a long time to get over the most recent online privacy violation incident.	2.24	1.2	1	5
Internet activities	web_1	Receiving and sending e-mails	4.01	1.04	1	5
	web_2	Using chat/instant message services (e.g., Messenger, WhatsApp, Viber)	4.13	1.05	1	5
	web_3	Downloading music and/or movies	2.45	1.23	1	5
	web_4	Playing online games	2.34	1.34	1	5
	web_5	Paying bills/e-banking	3.18	1.41	1	5
	web_6	Attending courses online	2.32	1.41	1	5
	web_7	Online shopping	2.5	1.28	1	5
	web_8	Live streaming and/or watching multimedia content (e.g., YouTube, online radio)	3.44	1.19	1	5
	web_9	Making audio/video calls and/or meetings (e.g., Skype, Zoom)	2.86	1.27	1	5
	web_10	Using social networks (e.g., Facebook, Twitter, Instagram, TikTok)	3.65	1.34	1	5
	web_11	Following daily news online	3.75	1.05	1	5
	web_12	Using search engines to find information (e.g., Google)	4.3	0.84	1	5
	web_13	Searching for maps and driving directions	2.87	1.15	1	5
	web_14	Using online forums	2	1.1	1	5
	web_15	Using public services available online (e.g., e-građani, filing taxes online, e-upisi, e-dnevnik, postani student)	2.76	1.24	1	5
Internet skills	skill_1	I can use a browser (e.g., Chrome, Firefox, Safari) to navigate the Internet.	4.39	0.91	1	5
	skill_2	I can register a new e-mail address (e.g., Gmail) or social network (e.g., Facebook) account.	4.26	1.05	1	5
	skill_3	I can work with/edit bookmarks.	3.85	1.35	1	5
	skill_4	I can save content from websites to my device.	3.71	1.39	1	5
	skill_5	I can administer a website.	2.54	1.44	1	5
	skill_6	I can create a website.	2.15	1.36	1	5
Personality traits – extraversion	pt_1	I see myself as someone who is reserved.	2.57	1.01	1	5
	pt_6	I see myself as someone who is outgoing, sociable.	3.97	0.92	1	5
Personality traits – agreeableness	pt_2	I see myself as someone who is generally trusting.	3.55	0.83	1	5
	pt_7	I see myself as someone who tends to find fault with others.	1.91	0.92	1	5
Personality traits – conscientiousness	pt_3	I see myself as someone who tends to be lazy.	2.08	1.04	1	5
	pt_8	I see myself as someone who does a thorough job.	3.95	0.84	1	5
Personality traits – neuroticism	pt_4	I see myself as someone who is relaxed and handles stress well.	3.41	0.99	1	5
	pt_9	I see myself as someone who gets nervous easily.	2.55	1.07	1	5
Personality traits – openness	pt_5	I see myself as someone who has artistic interests.	3.36	1.2	1	5
	pt_10	I see myself as someone who has an active imagination.	3.35	1.17	1	5

Latent construct	Item	Description	Mean	St. dev.	Min.	Max.
Optimism	opt_1	I always look on the bright side of things.	3.73	0.84	1	5
	opt_2	I'm always optimistic about my future.	3.75	0.87	1	5
	opt_3	In general, things turn out all right in the end.	3.56	0.8	1	5
Pessimism	pes_1	Rarely do I expect good things to happen.	2.38	1.05	1	5
	pes_2	Things never work out the way I want them to.	2.48	0.96	1	5
	pes_3	Better to expect defeat: then it doesn't hit so hard when it comes.	2.65	1.03	1	5
Self-esteem	se_1	I have high self-esteem.	3.72	0.89	1	5
Self-efficacy	sef_1	It is easy for me to stick to my aims and accomplish my goals.	3.73	0.82	1	5
	sef_2	Thanks to my resourcefulness, I know how to handle unforeseen situations.	3.87	0.79	1	5
	sef_3	I can solve most problems if I invest the necessary effort.	4.11	0.75	1	5
	sef_4	I can remain calm when facing difficulties because I can rely on my coping abilities.	3.89	0.83	1	5
Social trust	st_1	In general, I trust people.	3.39	0.93	1	5
	st_2	In general, I trust state public institutions.	2.35	1.05	1	5
	st_3	In general, I trust local/municipal public institutions.	2.5	1.03	1	5
	st_4	In general, I trust my local community (e.g., neighbors, people that surround me).	3.32	1.03	1	5
Online privacy awareness	oaw_1	I keep myself updated about privacy issues and the solutions that companies and the government employ to ensure our online privacy.	2.85	1.05	1	5
	oaw_2	Websites seeking information about me should disclose the way the data are collected, processed, and used.	4.12	1.07	1	5
	oaw_3	A good online privacy policy should have a clear and conspicuous disclosure.	4.31	0.88	1	5
General Internet attitude scale	gias_1	In general, I have a positive attitude toward the Internet.	3.79	0.84	1	5
Internet benefits	bnf_1	In general, my need to obtain certain information or services from the Internet is greater than my concern about online privacy.	3.34	0.98	1	5
	bnf_2	The greater my interest to obtain a certain information or service from the Internet, the more I tend to suppress my online privacy concerns.	2.92	1.03	1	5
Digital anxiety	da_1	Digitalization is a real threat to privacy.	3.45	1.09	1	5
	da_2	I am easily frustrated by increased digitalization in my life.	2.99	1.15	1	5
Digital public services	dps_1	Assuming I have access to digital public services, I intend to use them.	3.93	1.09	1	5
	dps_2	If I had access to digital public services, I predict that I would use them.	3.92	1.1	1	5
Local digital public services	ldps_1	Assuming I have access to digital public services in my city or municipality, I intend to use them (e.g., smart parking system, web cameras, free WiFi, waste management, e-tickets in public transport, ...).	3.94	1.06	1	5
	ldps_2	If I had access to digital public services in my city or municipality, I predict that I would use them (e.g., smart parking system, web cameras, free WiFi, waste management, e-tickets in public transport, ...).	3.95	1.05	1	5
Online privacy concern	opc_1	I am concerned about my online privacy.	3.31	1.03	1	5
	opc_2	I am concerned about extensive collection of my personal information over the Internet.	3.69	1.08	1	5
	opc_3	I am concerned about my privacy violation when using the Internet.	3.5	1.07	1	5
Degree of regulatory control	reg_1	The existing laws in my country are sufficient to protect peoples' online privacy.	2.52	1.01	1	5
	reg_2	The government is doing enough to ensure that citizens are protected against online privacy violations.	2.37	1.03	1	5

Latent construct	Item	Description	Mean	St. dev.	Min.	Max.
Sharing private information online	sh_1	I don't mind sharing private information publicly on the Internet.	2.22	1.11	1	5
	sh_2	I don't mind posting my current location publicly on the Internet.	2.28	1.24	1	5
	sh_3	I don't mind posting with whom I am at the moment publicly on the Internet.	2.37	1.28	1	5
	sh_4	I see no problem in sending my credit card data when buying online.	2.31	1.26	1	5
Protective behavior	pb_1	I give fictitious responses to avoid giving websites real information about myself.	2.08	1.09	1	5
	pb_2	I use another name or e-mail address when registering on a website without divulging my real identity.	2.05	1.22	1	5
	pb_3	When registering on a website, if possible, I only fill in data partially.	3.27	1.27	1	5
	pb_4	I try to eliminate cookies that track my Internet activities.	3.17	1.25	1	5
	pb_5	I try to disguise my identity when browsing (private browsing option).	2.49	1.29	1	5
	pb_6	I refuse to provide personal information to untrustworthy websites.	3.91	1.25	1	5

Abbreviations

F – filter questions

PV – privacy violation description

RES – resilience to online privacy violation

ATT – behavior and attitude change after online privacy breach

T – time spent online for private and work-related reasons

WEB – diversity of online activities

SKILL – Internet skills

PT– personality traits

V – personal values

OPT – optimism

PES – pessimism

SS – social support

SE – self-esteem

SEF – self-efficacy

OAW – online privacy awareness

ST – social trust

GIAS – general Internet attitude scale

BNF – perceived online benefits

DA – digitalization anxiety

DPS – digital public services

LDPS – local digital public services

OPC – online privacy concern

REG – degree of regulatory control

SH – sharing private information online

PB – protective behavior

IT – intent to adopt new technologies

EBUY – online purchases

D – demographics

OPVI – online privacy violation incident

PV_ser – privacy violation seriousness

DESI – digital economy and society index

ISBN 978-953-6030-60-6
9 789536 030606