Sofia Ranchordas and Malou Beck

57 Vulnerability

Abstract: This chapter explores definitions and theories of vulnerability, emphasizing its complexity, elusive nature, and the impact of digitalization on exacerbating vulnerabilities in the public sector and the criminal justice system. It examines a conceptual understanding of administrative vulnerability and draws on existing scholarship theorizing vulnerability as exposure to harm, individual and particular, universal and inherent, and multi-layered.

Keywords: vulnerability, digitalization, criminal justice, public sector governance, inequality

Introduction

The academic conceptualization of vulnerability first emerged in the early 1980s in the study of natural disasters (Delor and Hubert, 2000: 1561). Today, vulnerability is explored in multiple sciences and is used in both the analog and digital contexts. In cybersecurity, any flaw in an organization's internal controls, system procedures, or information systems can be regarded as a 'vulnerability.' Cybersecurity vulnerabilities affect individuals, businesses, and nation states, and research has shown that some countries (e.g., India and South Korea) are particularly vulnerable to cyber threats (Subrahmanian et al., 2015). Similarly, in organizational studies, vulnerability has also been connected to the identification of threats and risks within corporations. However, in this field of study, vulnerability has also been approached from a management perspective: originally regarded as a weakness, vulnerability in management equates nowadays to empathic and humble leadership (Brown, 2018).

In law and criminology, vulnerability is primarily associated with features of specific groups. For instance, persons with disabilities, migrants, or children are commonly considered vulnerable. The subfield of zemiology draws attention to the meaning of vulnerability in relation to social harms, identifying structural disadvantages, systemic injustices, and unequal power structures (Canning and Tombs, 2021). In law, vulnerability is traditionally connected to belonging to a certain group (e.g., children) and as such, vulnerable citizens are awarded additional legal protection when they cannot exercise their rights. Vulnerability theories developed in the context of legal feminist studies depart from this position. They challenge the existence of 'an average citizen' free from vulnerability. Instead, Fineman (2008), for example, suggests that vulnerabil-

Disclaimers and acknowledgments: This research was funded by the Netherlands Organization for Scientific Research (NWO) in the context of the NWO-Vidi Project 'Vulnerability in the Digital Administrative State' led by Sofia Ranchordas.

 https://doi.org/10.1515/9783111062037-058

ity is universal and inherently human. Thus, all individuals can be vulnerable due to an ever-present risk of being harmed: what varies is a person's degree of vulnerability. Interestingly, this position is mirrored in the etymology of the term 'vulnerable.' Originating from the Latin term *vulnus* or wound (Malgieri and Niklas, 2020: 3), vulnerability depicts "the fragile and contingent nature of personhood" (Beckett, 2006: 3). To illustrate, senior citizens with limited digital literacy may be vulnerable online due to their higher risk of being targeted by cybercriminals (see Cybercrime by Holt and Holt). However, young people who have profound digital skills may also encounter moments of digital vulnerability. This can occur when they face personal challenges, such as a traumatic life event that temporarily reduces their ability to navigate complex digital tools independently (Calderón Gómez, 2019). While consensus exists on vulnerability as the susceptibility to be harmed, the broader aspects of the concept remain elusive.

This contribution explores key definitions and theories of vulnerability and their significance in the digital context. In criminology, vulnerability provides a valuable tool to reveal and attend to social inequalities and unjust societal structures. In addition, the concept sheds light on the human dimension in today's digital society.

Theories of vulnerability: the state-of-the-art

While progress has been made in protecting vulnerable groups, the definition of vulnerability remains a fragmented exercise (Schroeder and Gefenas, 2009). Definitions of vulnerability can be vague and biased, especially when tied to particular identity groups. Moreover, the term 'vulnerability' is often misused in academia, popular science, and media, jeopardizing its intended meaning and protective value. Four conceptualizations of vulnerability stand out, namely (i) exposure to harm; (ii) individual particularities; (iii) the universal character of vulnerability; and (iv) the existence of multiple layers of vulnerability.

First, vulnerability can be defined by reference to being "exposed to the possibility of being attacked or harmed, either physically or emotionally" (Schroeder and Gefenas, 2009: 114). This implies that once an individual has been harmed, they are no longer vulnerable. While exposure to harm is the external dimension of vulnerability, the inability to defend oneself against harm its the internal element (Delor and Hubert, 2009). For instance, citizens with limited digital literacy may be more exposed to digital harms such as identity theft. As such their internal vulnerability manifests itself in the reduced capacity to protect their personal data against such this type of cybercrime.

A second strand of scholarship associates vulnerability with *particularity*, qualifying individuals as vulnerable based on specific situations and socio-economic contexts. Despite being widespread in legal and criminology scholarship, the *particular* approach to vulnerability has been critiqued due to the risk of profiling, stigmatization, and grouping people as vulnerable (Heri, 2021). This has been common in the context of hate crimes which focuses on the collective experiences of minority groups and their

victimization (Chakraborti and Garland, 2012). While this particularity-qualification is practical from a policy perspective, this label does not account for the complexity and fluidity of vulnerability, individual needs, and may thus "not reliably protect many individuals from harm" (Levine et al., 2004: 44). This is particularly true in the digital realm, where data pertaining to individuals within the same population groups may be categorized differently, despite their shared vulnerabilities (Malgieri and Niklas, 2020).

The third set adopts a ***universal*** approach to vulnerability, embracing Martha Fineman's theory of the ubiquitous character of vulnerability (Fineman, 2008, 2010, 2019a). Fineman argues that human vulnerability is defined by universality and is "inherent to the human condition" (Fineman, 2008: 1). Fineman's feminist legal notion of a *universal* vulnerable legal subject assumes that vulnerability is not centered around specific groups, rejecting the understanding that vulnerability can be classified based on individuals' particularities such as race, gender, or ethnicity (Fineman, 2010: 253). Scholarship has interpreted the departure from vulnerability as a categorization of certain 'weak' groups or 'victims' as a positive development in the combat against the stigma of the term (Mackenzie, 2014; Cole, 2016; Gilson, 2011; Malgieri and Niklas, 2020; Kohn, 2014). In Fineman's work, being human means being vulnerable. Vulnerability is converted into a feature that cannot be eliminated and is often beyond human control (Fineman 2019b: 53; Fineman, 2008: 9). Thus, Fineman defines vulnerability as "the unavoidable susceptibility to change, both positive and negative, in our physical wellbeing that we experience over the life course"(Fineman 2019b: 57). Moreover, Fineman advocates for a responsive state, criticizing today's neoliberal state which places excessive focus on the liberty and autonomy of the individual forgetting human dependency and vulnerability (Fineman, 2010). In the digital context, such universal approach to vulnerability entails an acknowledgement that all citizens can be harmed by the digitalization of law enforcement or the criminal justice system. Thus, vulnerability can also be inflicted on individuals that fall out of common vulnerability categories. For instance, vulnerability arising from cyber threats, such as online scams or e-mail phishing, is not limited to specific population groups.

The fourth strand of scholarship regards vulnerability as a complex, fluid, and multi-layered concept, thus building upon universal perceptions but refining it by explaining how some individuals may be confronted with more layers of vulnerability than others (Luna, 2009: 128). Luna's notion of vulnerability rejects the stigmatization and simplistic categorization of individuals in vulnerable groups (Luna, 2009: 124). To illustrate, being a single mother of four children can constitute a layer of vulnerability. Low income and health problems, when present, will add layers to the vulnerability experienced by this mother, leading to 'cascade effects' (Luna, 2019: 91). The existence of multiple cumulative layers of vulnerability is often considered in sentencing in criminal law. The assessment of the presence of these layers is thus relevant to evaluate the vulnerability of individuals in criminal investigations.

Sources of vulnerability

Scholarship on vulnerability has sought to understand vulnerability through its many *sources* and *states.* Vulnerability can be permanent (e. g., physical disabilities) or temporary (e. g., a life event such as the death of a loved one). Vulnerability sources can also be inherent or situational: *inherent sources* of vulnerability pertain to the human condition (age, gender, health), while *situational sources* are more context-specific and often "caused or exacerbated by social, political, economic or environmental factors" (Mackenzie, 2014: 39). These sources of vulnerability do not exist in isolation, as they can be closely intertwined and can reinforce or trigger one another (Mackenzie, 2014). For example, individuals experiencing poor mental health may be more vulnerable to emotional distress from online harassment. Moreover, inherent and situational sources of vulnerability can be temporary or long-lasting and can take dispositional or occurrent forms (Mackenzie, 2014: 39). In addition, part of the situational vulnerability sources are pathogenic vulnerabilities, which are inflicted through structural disadvantage and thus result from "and from social domination, oppression, or political violence" (Mackenzie, 2014: 39). Such pathogenic vulnerabilities can, for instance, occur in discriminatory and racially biased algorithms in criminal sentencing (see Sentencing and Risk Assessments by Ugwudike). When such algorithms mirror long standing structural disadvantage and unequal power structures, they give rise to pathogenic vulnerabilities for such oppressed population groups.

Our position and administrative vulnerability

While there are various perspectives on vulnerability, we adopt a socio-legal approach and understand vulnerability as a universal, individual, and multi-layered concept. This approach matches partially with vulnerability concepts in the field of digital criminology. Vulnerability is the susceptibility of being placed in a position of economic, social, ecological, or legal disadvantage with potential harm as the result. In our administrative law and sociolegal scholarship, we develop the term *'administrative vulnerability'* to convey the inability to critically engage with digital government, bureaucracy, and exercise rights before government on equal terms. Administrative vulnerability is a fluid concept that encompasses intrinsic and situational vulnerability. It conveys a state of inequality, i. e., citizens experiencing situational vulnerability will not be able to exercise their rights on equal terms. Administrative vulnerability is problematic for four reasons: first, citizens have rights before government and are entitled to receiving different types of assistance and public services; second, citizens typically do not have choice when it comes to the provision of public services as in many countries, the state is their sole provider; third, the relationship between state and citizens is inherently defined by power asymmetries; fourth, in a democratic society governed by the rule of law, citizens experiencing vulnerability can rightfully expect to be protected

rather than be harmed by government. Nowadays, public services and public assistance such as social welfare benefits are provided mainly through digital government in numerous high-income countries. For instance, citizen will be regarded as administratively vulnerable if digital government platforms do not provide easy access to such services.

Significant power asymmetries between citizens and governments typically define government transactions, particularly criminal investigations and the gathering of digital evidence. However, some situations will place individuals in more vulnerable conditions than others, depending on the existing layers of vulnerability, structural disadvantage, and the specific relationship between citizens and the government. Furthermore, administrative vulnerability can occur in many different contexts of digital government, ranging from accessing and engaging with digital services to becoming victims to algorithms or automated decision-making systems. For instance, if individuals are unable to engage with digital tools, they can become vulnerable when unable to challenging decisions taken against them and, thus, accessing justice. Moreover, sentencing algorithms, surveillance systems and policing softwares can give rise to vulnerabilities if, for instance, racially biased learning data is used, ultimately resulting in discriminatory outcomes and fundamental rights violations (see Bias by Oswald and Paul).

While it is true that everyone can be vulnerable, not all citizens are susceptible to experience vulnerability at the same level. Our position acknowledges that some individuals are predisposed to particular layers of vulnerability because of endogenous or exogenous sources of vulnerability or risk factors. For example, individuals with limited digital literacy may be more susceptible to different forms of cybercrime such as phishing scams, identity theft, or online fraud. The cumulation of layers of vulnerability should also be considered as it can have de facto a punitive effect on citizens, underlining the urge to draw attention to it in critical criminology scholarship. For example, welfare recipients who experience multiple layers of vulnerability (low income, criminal record, low literacy, and limited digital skills) may be at higher risk of being targeted by welfare investigations due to algorithmic biases. At the same time, they may inadvertently confirm this risk factor by making unintentional mistakes when filling in forms or providing inaccurate information to the government due to their limited knowledge and skills. As the state unintentionally but directly inflicts administrative vulnerability, this concept also acknowledges Fineman's idea that the state should be responsible for combatting and accounting for it.

Critical criminology scholarship would benefit from a layered approach and the departure from negative and stigmatizing perceptions of vulnerability that label entire population groups as vulnerable. These perceptions do not always entail a critical inquiry into the experience of these populations and how they may be stigmatized because of the 'vulnerability-label.' Instead, all individuals are prone to administrative vulnerability and carry layers that can make them susceptible to it. This underlines the universal and complex nature of the concept as defined in Fineman's vulnerability theory.

Vulnerability, criminology, and the digital

With the growing use of technology (e.g., biometrics, big data, AI) in predictive policing, welfare fraud investigations, and criminal investigations, some groups have become more vulnerable to biases and the risk of wrong accusations (Susser, 2021). The use of biometrics to govern, regulate, and police by identity has, for instance, proven problematic to ethnic minorities (Skinner, 2020). Ethnic minorities are often discriminated against by predictive systems that score them negatively, suggest they will commit crimes and welfare fraud more often, and surveil them more closely than other segments of the population (Ferguson, 2017: 1109). Biometric identification typically affects these groups negatively as these groups are more regularly selected for random biometric identification at airports, train stations, and other public spaces (Magnet, 2011). The compromise text of the AI Act which will regulate a wide range of AI systems in the European Union, aims to impose future limits on real-time biometric identification in public spaces. This is crucial to avoid that ethnic minorities experience additional vulnerability in criminal investigations, particularly when there have been several documented cases of wrongful incrimination. However, a more profound solution here would entail the elimination of unjust power and opportunity structures and structural disadvantage to ethnic minorities as the root cause of biased datasets and vulnerability.

Furthermore, debates surrounding the emergence of e-courts and a digitalized criminal justice system have created new digital vulnerabilities for various groups (see Online Courts by Mentovich and Rabinovich Einy). While traditionally, there has been a dichotomy between the victim as the vulnerable and the offenders as the party inflicting vulnerabilities on individuals (Green, 2012), recent digital advancements have urged us to rethink such narrow understandings of vulnerability. For instance, the use of audio-visual communication tools in the context of courts has given rise not only to new vulnerabilities for victims, their networks, and crime witnesses but also to offenders and incarcerated individuals. For instance, Parsons and Sherwood (2016) claim that communication and information provision can be challenging for detained individuals with learning disabilities. This can have far-reaching consequences and even lead to detrimental miscarriages of justice. While such issues are already evident in paper-based communication channels (Parsons and Sherwood, 2016: 569), digitalizing such processes risks exacerbating such vulnerabilities.

In addition, courts have not only given rise to vulnerability related to access to justice, but the use of remote access technologies in courts also raises questions regarding power relations, justice, and fairness (McKay, 2022: 74). Vargas et al. (2019) argue that citizens' e-contact with the criminal justice system has given rise to new digital vulnerabilities through the risk of data breaches in the context of police-dispatcher radio communication, primarily affecting racial minorities in disadvantaged neighborhoods. Thus, "citizen vulnerability occurs not only physically during police stops on the streets or country courts, but also digitally across cyberspace and radio waves" (Vargas et al.,

2019: 74). Notwithstanding, in the criminal justice system, individuals generally find themselves in vulnerable positions, which can be exacerbated through digital tools. Prevailing attributes that render individuals vulnerable in bail decisions are race, age, sex, and socioeconomic status (Hughes et al., 2022). In conclusion, the digital dimension of law enforcement and judicial procedures exposes individuals to additional vulnerabilities and thus potential harm.

Conclusion

Vulnerability is a complex, universal but also individual, multi-layered concept. To be human is to be vulnerable and each and every one of us can be vulnerable in our own way. While there has been progress in the protection of vulnerable groups, commonly used definitions of vulnerability remain restricted by their connection to closed groups and categories. This contribution highlighted four central conceptualizations of vulnerability based on the notions of (i) exposure to harm; (ii) individual particularities; (iii) the universal character of vulnerability; and (iv) the existence of multiple layers of vulnerability. Furthermore, we explained that vulnerability stems from different sources, such as inherent, situational, or pathogenic sources, and can manifest itself in occurrent, dispositional, temporary, or permanent form (Mackenzie, 2014). While the digitalization and automation of the public sector and criminal justice system has given rise to new types of vulnerabilities, such as identity fraud, problematic digital evidence practices, cybercrimes, predictive fraud risk algorithms, or access to e-courts, these conceptualizations of vulnerability sources remain relevant and applicable. We argued that vulnerability is a *state* that every individual can experience, rather than a *status* or label that is given to underprivileged groups. While some individuals are more exposed to different layers of vulnerability and may thus require additional protection against for example cybercrime or online harassment, the state should be mindful that vulnerability is an inherent feature of human identity.

Moving forward, scholars, policymakers, and governments should be attentive to the impact of the digital transformation on individuals. The digital creates a context in which existing layers of vulnerability become more salient and new layers such as digital and algorithmic illiteracy emerge.

Suggested reading

Dehaghani, R., Fairclough, S., & Mergaerts, L. (eds.) (2023). *Vulnerability, the Accused, and the Criminal Justice System: Multi-jurisdictional Perspectives.* London: Routledge.

Fineman, M., & Spitz, L. (eds.) (2024). *Law, Vulnerability, and the Responsive State Beyond Equality and Liberty.* London: Routledge (forthcoming)

Green, S. (2012). Crime, victimisation and vulnerability. In S. Walklate (ed.), *Handbook of Victims and Victimology* (pp. 107–134). Cullompton: Willan

Hickey, J. (ed.) (2023). *The Foundations of Vulnerability Theory: Feminism, Family, and Fineman* (1st ed.). London: Routledge.
Malgieri, G. (2023). *Vulnerability and Data Protection Law.* Oxford: Oxford University Press.
Taylor, S. (2022). 7: The problem with the current agenda: Focus on vulnerability. In *Hate Crime Policy and Disability* (pp. 144 – 167). Bristol: Bristol University Press. Available from: < https://doi.org/10.51952/9781529217902.ch007> [Accessed 03 August 2023]

References

Beckett, A. (2006). *Citizenship and Vulnerability: Disability and Issues of Social and Political Engagement.* Basingstoke: Palgrave MacMillan.
Brown, B. (2018). *Dare to Lead: Brave Work. Tough Conversations. Whole Hearts.* London: Random House.
Calderón Gómez, D. (2019). Technological capital and digital divide among young people: An intersectional approach. *Journal of Youth Studies*, 22(7), 941 – 958.
Canning, V., & Tombs, S. (2021). *From Social Harm to Zemiology: A Critical Introduction.* London: Routledge.
Chakraborti, N., & Garland, J. (2012). Reconceptualizing hate crime victimization through the lens of vulnerability and 'difference'. *Theoretical Criminology*, 16(4), 499 – 514.
Cole, A. (2016). All of us are vulnerable, but some are more vulnerable than others: The political ambiguity of vulnerability studies, an ambivalent critique. *Critical Horizons*, 17(2), 260 – 277
Delor, F., & Hubert, M. (2000). Revisiting the concept of 'vulnerability'. *Social Science & Medicine*, 50(11), 1557 – 1570.
Ferguson, A. G. (2017). Policing predictive policing. *Washington University Law Review*, 94(5), 1109 – 1189.
Fineman, M. A. (2008). The vulnerable subject: Anchoring equality in the human condition. *Yale Journal of Law & Feminism*, 20, 1 – 24.
Fineman, M. (2010). The vulnerable subject and the responsive state. *Emory Law Journal*, 60, 251 – 267.
Fineman, M. A. (2019a). Vulnerability and social justice. *Valparaiso University Law Review*, 53, 341 – 369
Fineman, M. A. (2019b). Vulnerability in law and bioethics. *Journal of Health Care for the Poor and Underserved*, 30(5), 52 – 61.
Gilson, E. (2011). Vulnerability, ignorance, and oppression. *Hypatia*, 26(2), 308 – 332.
Green, S. (2012). Crime, victimisation and vulnerability. In S. Walklate (ed.), *Handbook of Victims and Victimology* (pp. 107 – 134). London: Routledge.
Heri, C. (2021). *Responsive Human Rights: Vulnerability, Ill-treatment and the ECtHR.* Oxford: Hart Publishing.
Hughes, D., Colvin, E., & Bartkowiak-Théron, I. (2022). Police and vulnerability in bail decisions' *International Journal for Crime, Justice and Social Democracy*, 11(3), 122 – 138.
Kohn, N. A. (2014). Vulnerability theory and the role of government. *Yale Journal Law & Feminism*, 26, 1 – 28.
Levine, C., Faden, R., Grady, C., Hammerschmidt, D., Eckenwiler, L., & Sugarman, J. (2004). The limitations of "vulnerability" as a protection for human research participants. *The American Journal of Bioethics*, 4(3), 44 – 49.
Luna, F. (2009). Elucidating the concept of vulnerability: Layers not labels. *IJFAB: International Journal of Feminist Approaches to Bioethics*, 2(1), 121 – 139.
Luna, F. (2019). Identifying and evaluating layers of vulnerability – a way forward. *Developing World Bioethics*, 19(2), 86 – 95.
Mackenzie, C. (2014). The importance of relational autonomy and capabilities for an ethics of vulnerability. In C. Mackenzie, W. Rogers, & S. Dodds (eds.), *Vulnerability: New Essays in Ethics and Feminist Philosophy* (pp. 33 – 59). New York: Oxford University Press.
Magnet, S. (2011). *When Biometrics Fail: Gender, Race, and the Technology of Identity.* Durham, NC: Duke University Press.

Malgieri, G., & Niklas, J. (2020). Vulnerable data subjects. *Computer Law & Security Review*, 37, 105415.

McKay, C. (2022). Remote access technologies, clinical evaluations of people-in-prison and digital vulnerability. *Recht der Werkelijkheid /Journal of Empirical Research on Law in Action*, 43(2), 68 – 88.

Parsons, S., & Sherwood, G. (2016). Vulnerability in custody: Perceptions and practices of police officers and criminal justice professionals in meeting the communication needs of offenders with learning disabilities and learning difficulties. *Disability & Society*, 31(4), 553 – 572

Schroeder, D., & Gefenas, E. (2009). Vulnerability: Too vague and too broad? *Cambridge Quarterly of Healthcare Ethics*, 18(2), 113 – 121.

Skinner, D. (2020). Race, racism and identification in the era of technosecurity. *Science as Culture*, 29(1), 77 – 99.

Subrahmanian, V. S., Ovelgonne, M., Dumitras, T., & Prakash, B. A. (2015). *The Global Cyber-Vulnerability Report.* Cham: Springer.

Susser, D. (2021). Predictive policing and the ethics of preemption. In B. Jones & E. Mendieta (eds.), *The Ethics of Policing: New Perspectives on Law Enforcement* (pp. 268 – 292). New York: NYU Press.

Vargas, R., Preto-Hodge, K., & Christofferson, J. (2019). Digital vulnerability: The unequal risk of e-contact with the criminal justice system. *RSF: The Russell Sage Foundation Journal of the Social Sciences*, 5(1), 71 – 88.