Ermoshina Ksenia and Musiani Francesca (2022) Concealing for Freedom: The making of Encryption, Secure Messaging and Digital Liberties. Manchester: Mattering Press

Samuele Fratini
samuele.fratini@phd.unipd.it

Whereas Governance scholars have always been committed to the analysis of policy issues, political institutions and regulation processes, the growing digitalization of society has turned the table greatly. The cyberspace is now submitted to a variety of national jurisdictions and the local and the global are inherently intertwined. Under these circumstances, social actors are no longer able to exert direct control over the digital flow of information. Power struggles are thus relocated at the material level, and Internet Governance needs to learn STS: the technical components of the digital infrastructures have become more political than ever. In their book, *Concealing for Freedom: The making of Encryption, Secure Messaging and Digital Liberties*, Ksenia Ermoshina and Francesca Musiani maintain that, since the Snowden revelations, encryption is among the most political features of digital technology, and its comprehension needs to come along its socio-cultural situalization. Based on the empirical analysis of the end-to-end encrypted mailing and messaging applications (i.e., Signal, LEAP/Pixelated and Briar), this work represents the "the first book-length endeavour" (p. 35) dealing with encryption as a political matter from an STS perspective. The concrete output is "an analytical portrait of the field of encrypted secure messaging" (p. 60). Yet, in terms of social sciences, this work is a much-needed theoretical and methodological contextualization of how controversies take place in the digital age.

After a sixty-page introduction, the first chapter problematizes the concepts of threat, considering that users perceive to be spied by different antagonists. Depending on the adversary, different aspects of their identity are jeopardized: "users perceive themselves […] as possessing a set of 'profiles' or 'personas'" (p. 66). In the online domain, risk and security are relational concepts. By interviewing digital security trainers, Ermoshina and Musiani deliver a detailed exploration on the use they make of threat modelling and risk assessment. While the former "enables development teams to examine the application 'through the eyes of a potential adversary' to identify major security risks", the latter is used "in order to analyze the chance of a threat being realized" (p. 70). This allowed trainers to organize their sessions in the light of the assumed threat. Furthermore, users are categorized based on their likelihood to be exposed to danger, and then the threat is identified.

The first chapter is followed by what the authors call an 'analytical triptych', whose aim is "to provide an analysis of different architectural choices and their impact on the configuration – social and economic as well as technical – of encrypted messaging tools" (p. 89). The first case study is the Signal protocol, paradigmatic example of a centralized architectural model. The analysis is an opportunity to frame centralization as a form of "control by design" (p. 90), because it allows developers to respond

to technical challenges, needs of updates and uncertainty quicklier and without outsourcing the function to third-party developers. The following analysis is instead devoted to the peer-to-peer model. Discussing the case of Briar, peer-to-peer, i.e., the deployment of a technical architecture made up of distributed networks, seems to promise a softer degree of both governmental and corporate control. Great interest for such an implementation is shown by users and developers from high-risk countries, e.g., Russia. Nevertheless, while de-centralization remains a widely contested concept, and many definitory attempts diverge, its application to encrypted messaging has been greatly overlooked. The chapter argues that the causal relation between de-centralized architecture and horizontal modes of governance has been too rapidly assumed: according to the authors, this is heavily linked with the diverging definitions which different social groups attach to the notion of de-centralization. The triptych ends with federative models of construction by reconstructing the historical debate around the concept. After providing an in-depth consideration of the technical advantages (i.e., alleviating personal responsibility of developers by enabling the users to choose among a variety of options, spreading interoperability, promoting localism and resilience) and disadvantages (i.e., the difficult harmonization and updating of all the different implementations), the authors make clear how federated protocols are framed as both architectural choices and social experiment (p. 62).

After a hundred pages covering different architectural solutions in messaging and emails, the fifth chapter tries to make some order by addressing the issue of categorization. Drawing on the Star and Bowker's (1999) well-known book on classification, the authors are aware that categorization takes up political, ethical and cultural significance when applied to technologies that are under the way of stabilization. Case study for this purpose is the 2014 Secure Messaging Scorecard (SMS) released by the Electronic Frontier Foundation, through which different messaging and mailing applications have been evaluated in terms of security. Of particular interest in the debated sparked around such a classification: because the notions of security and privacy are contested even within apparently like-minded communities, attempts of classification emerge as process of negotiation of meanings resulting in an action which co-shapes the system it tries to make sense of.

The book is concluded with some developments of the considerations advanced throughout the long introduction. The idea of encryption as infrastructural site of socio-political struggle is remarked, and the authors draw a line between two narratives and two distinguished evolutions: as encryption is linked with both civil liberties and terrorism, its massive implementation has been pursued for restoring trust in digital technologies as well as for opportunistic purposes (p. 205). The chapter is closed by exposing some implementing solutions for digital security, connecting it with supranational legislative framework, e.g., the General Data Protection Regulation (GDPR), and with the very same architectural choices.

Although the book's contribution is devoted to Internet Governance, it collaterally enriches the STS debate. While bringing the political into the technical, conceptualizing encryption as a site of struggle, it conversely implies the reverse connection between those two dimensions. How does the 'cryptographic turn' (p. 210) re-shape political and economic trials between state and non-state actors? As it is now well-established in the STS research tradition, technology is deemed to be embedded in the social texture, and it cannot be understood in terms of causal dependence: when political struggles re-frame the purposes of encryption, encryption re-shape the forms of political struggles, and the final part of the book re-conceptualizes the most urgent social and political issues in the light of the discussed breakthroughs.

In terms of limitations, the readers should be aware that the book does not provide any particularly revolutionary concepts to the STS field of study, as it is rather aimed at applying the STS theoretical background to re-shape the field of Internet Governance. This virtuous mixture is oriented to, as the authors themselves declare, the ongoing discussion around "several pressing Internet Governance issues" (p. 19): approaching this work from an STS point of view is less fruitful in terms of theoretical production, while it is rather

suitable to explore a particularly cogent field of interrelation between two academic traditions. Future research starting from the same background may address technical features other than encryption and attempt to unfold its encoded sociomaterial implications. *Concealing for Freedom* is then also a toolkit for those new scholars who are willing to dive into the infrastructural turn in the Internet governance, as this contribution offers a precise blueprint of how to conduct an infrastructural analysis from a sociomaterial perspective with the objective of rendering its inherent complexity.

References

Bowker GC and Star SL (2000) *Sorting things out: Classification and its consequences*. Cambridge: The MIT press.