Dada Rivista di Antropologia post-globale, semestrale n. 1, Giugno 2026

Counter-surveillance as a crime or as resistance? Julian Assange and the case of *Wikileaks*

Vincenzo Scalia

Abstract

Relational surveillance makes the relation between the surveilled and the surveillants more and more ambiguous. The former, by surfing in the web, are able to gather those informations about the crimes of the powerful that can increase the awareness of public opinion about abuses committed by those who hold either economic or political power. Julian Assange and *Wikileaks*, who used their technological skills to make public opinion aware about tortures, secret prisons, massacres, were criminalized by the American government. Chelsea Manning was arrested and convicted. Assange faced a 14 years judicial prosecution, which only ended last 26th of June. The case of Julian Assange shows that the internet is a field of political struggles: despite those in power who try to control people, restrict the use of the web, and criminalize those who make an alternative use of it, an open, unrestrained use of the web both controls power and reinforces democracy.

Keywords: surveillance, counter-surveillance, deviance, Assange, resistance

Introduction

On the 25th of June 2024, Julian Assange, the spokesman of *Wikileaks*, was released on bail from the British prison of Belmarsh, where he had been held in custody since the 11th of April 2019, under the request of extradition issued by the US government. Washington had indicted Assange for conspiracy, following a law dating back to 1935 (Maurizi, 2020), for disclosing classified governmental documents that revealed serious state crimes committed by the US government. Despite the charge of conspiracy had been declared arbitrary by the United Nation Panel on arbitrary detention in 2015, the British government zealously complied with the American requests. Police forces broke into the Ecuador Embassy in London, where Assange had been living as a refugee since 2012. An illegal act, followed by five years of cruel detention. Until the Australian journalist- activist agreed to plead guilty for a minor offence, whose conviction was the equivalent of the 5 years he had served in prison.

The story of Julian Assange rose a discussion about the use of the web. Whereas more institutional sources argued that he had violated classified information, putting the security of millions and was by this token guilty, others emphasized the importance of freedom of information. According to the latter, Julian Assange had just put in practice the fundamental rights of free speech and information. Consequently, his detention and possible deportation were a symptom of the current critical conditions of Western democracies. The detention of a person who informs the public on the ground of such crimes as treason sounds like an intimidation for those who want challenge current power relations by engaging in radical practices, that is a criminalization of dissent (Vegh Weiss, 2021). Or, if one follows a more liberal approach, the restriction of the freedom of speech entails the risk of deteriorating the fabric of Western democracies.

On the other hand, if one scrolls through the comments some activists made on the social network, it is possible to find many negative comments about the decision of Julian Assange to plead guilty for a minor crime in change of his release. I consider this idea as flawed, for two reasons. Firstly, because by pleading guilty Assange did not regret what he did, but he just admitted what he had done. Secondly, because the behavior of the Australian activist was not different from that of many militants of radical or revolutionary organizations, like armed groups in 1970s. A declaration of guilt does not imply that one legitimizes the existing laws. It is rather the opposite case: an activist who plead guilty exposes the unfairness of the existing legal framework, that is established and enforced by the dominating social group.

The case of Julian Assange provides the chance to focus on two aspects, to be discussed in this paper: the first one concerns the discussion of the so-called *third space,* that is cyberspace (Tien, 2016). The fluid, impersonal nature of the internet, has risen concerns among some scholars, because of the increasing of control from above (Suvin, 2024), as well as on the possibility of reducing public discussion to a binary model and to restrict competition (Zuboff, 2019). Drawing on a definition forged by the Italian philosopher and novelist Umberto Eco (1963) I will call this approach as *apocalyptic.* According to these authors, pervasive control on the web by both economic and political actors creates a conformity of habits, expectations and values one cannot escape. Deviance becomes the consequence for those who do not comply with the requirements of the new controlling machine. More than this, it is not possible to act without being watched, so as to predict a new Orwellian model of society to take over. On the other hand, some authors, such as David Lyon (2016), on the trail of Michel Foucault (2007), emphasize the relational aspects of a network-shaped surveillance, wherein the surveilled not only provide information to the surveillant, but are also able to develop strategies of what I will define as *counter-surveillance.* Such definition, that recalls the *counter-power* 1970s social movements referred to (Ruggiero & Montagna, 2007), refers to three kinds of practices: the first

one, relates to the detection of surveillance strategies, such as the discovery of the Echelon network. The second is concerned to the documentation of brutalities, abuses and state crimes during public demonstrations, and it is usually defined as sous-veillance (Bradshaw, 2013). The third one consists of sabotage, and works as a direct answer to State crimes against civil population (like during the Gulf War). Counter-surveillance articulates in two stages: the first one is the breaking into the secrecy states advocate for sake of security. The second stage is that of making the public aware of State brutalities, so as to boost those shifts among public opinion that can bring about radical political changes.

The second aspect to be discussed, concerns the process of making and enforcing social norms and laws, out of which deviance is created, as well as the strategies of resistance to deploy against unfair rules promoted, approved by the dominating social groups. Assange is a deviant for the existing legal and political framework, and thus portrayed as a villain by the mainstream public opinion. The advocates of another social order, vice versa, have fought for the liberation of Julian Assange, arguing that he was a champion of civil liberties and prosecuted for his activities as an independent media activist. The conflict that developed around Julian Assange embodies the new power struggle around the control of information and of new technologies, as well as a fight against the repressive and authoritarian tendencies of dominating political actors. This paper will conclude that Assange's activism is a practice of counter-surveillance insofar as it keeps together both aspects, and that it should be part of a network of collective mobilization in the domain of IT and information. This is an innovative practice, that goes beyond sous-veillance, as it combines defensive and attacking tactics, and refuse the idea that all the actors who oppose neo-liberalism should work under the protection of secrecy.

Finally, it will be argued that there was a weak spot in the practice that Julian Assange and *Wikileaks* enacted. It is the isolation they suffered, for reasons of mutual misunderstanding. On the one hand, whereas they claimed they opposed neo-liberalism, they did not claim they were anti-capitalists. On the other hand, this created a misunderstanding by the many anti-capitalist movements, who thought that the prosecution of Julian Assange, as well as of *Wikileaks*, was just a matter of civil liberties, and not an anti-capitalist battle. I will argue that, both the centrality of the web in current capitalist production and the need to counterbalance the use of technology by the dominating powers, make it necessary for a stricter coordination and alliance by the different social movements, so as to make anti-capitalist resistance stronger and to work out a project of alternative society.

1.The internet as a battlefield: are *apocalyptics* wrong?

Since the internet broke out on the public stage, in early 1990s, its role in social relations, particularly in the structural changes in communication and interaction, discussions have arisen about the positive or negative role of the web. Some authors, such as Darko Suvin (2024, cit.), argue that the growing importance of IT in shaping daily life, will bring about an inevitable deterioration of the democratic fabric, as well as a decay of human skills. The binary logic underpinning algorithms will more and more reduce the space for in-depth knowledge and discussions. Though Suvin focuses his article on the development of artificial intelligence (AI), and of the reasons why it is necessary to afraid of it, his claims are based on a general fear of the expansion of new technology, on its negative effect on society. Social control and intellectual impoverishment march hand in glove with economic differences.

The view Suvin proposes marches hand in glove with the analysis that Shoshanna Zuboff (2019), developed in his major work. On the ground of the development of the so-called "platform-based capitalism" (Vecchi, 2019), Zuboff focuses on two aspects. The first relates to the triangular exchange of metadata between central governments, sub-contractors and private firms, which results into an invasion of the privacy of hundreds of millions of individuals, as their sensitive data are shared and used for private matters. Moreover, such a network of data exchanges, sets the standard for a very invasive control that paves the way for a new kind of Big Brother surveillance from above. Finally, in Zuboff's scheme, the overwhelming superiority of the digital majors in possessing and manipulating both the technology and the data, makes it easier to influence public opinion and to reduce the chances for a pluralistic public discussion over issues that are at stake in relation to the survival of Western democracies. Unlike Manuel Castells (2010) who cherishes the rise of network societies as a new opportunity for democracy and social inclusion more at large, Zuboff warns about the risk of current capitalism, whose surveillance-oriented attitude spans from political opinions to lifestyles, thus posing a danger to the fabric of civil society.

Both Zuboff's warning and Suvin's fear are to be taken into consideration, insofar as IT has been more and more used for purposes of both preventive and repressive surveillance. Ventura, Deflem and Miller (2005), have showed how the Project Carnivore, promoted by the US government since the enforcement of the Patriot Act, has consisted both of systematic violations of the due process of law and of targeting specific social groups like Muslims and political activists who opposed the War on Terror promoted by the American governments after 9/11. Moreover, the predictive models that developed out of the intelligence-led policing scheme (James, 2015; Radcliffe, 2016), base their pre-emptive purpose on the assumption that there are some individual, social groups and urban areas that are more "at risk" of delinquency than others. The use of IT becomes by this token a means to enhance the

production and reproduction of deviance, by labeling (Becker, 1963), the same, marginal individuals and social groups, thus making social inequalities stronger.

Despite the attitude to have a full control of society deployed by the dominating social groups, the processes of subjugation and repression are not so linear and inevitable as one might think. Firstly, the so-called third space, as the web is called (Geer, 2016), is not a uniform and linear context, as both individual and social conflicts are reproduced within its frame. Secondly, because there are always both potential and effective ways of resisting power, as well as of creating alternative practices and content. There are economic and political struggles that develop within the web, and the drawing of lines between legal and illegal, licit and illicit, law abiding and villains, depends on the outcome of these struggles. The criminalization of Julian Assange is a consequence of uneven force relations that, in present time, give governments and corporation the power both to produce and to enforce their rules. This point will be dealt with more in depth in the following session. But, in order to have a better understanding of it, a different definition of surveillance than that proposed by Zuboff and Suvin will be necessary.

2. An alternative, relational approach: *sous-veillance* to *counter-surveillance* and the criminalization of dissent

David Lyon (2016; 2018) defines contemporary surveillance as *relational,* developing horizontally, as opposed to the vertical kind of surveillance from below that developed during the modern State. The development of IT, as well as the transformations brought about by post-fordist capitalism (Ash, 1993), have produced a surveillance that works within the social fabric. On the one hand, the development of technology, allows traditional power agents, such as state, police and intelligence, to use sophisticated tools to control individuals. Metadata are stored into IT systems and eventually exchanged between contractors, market operators and political actors. The new model of surveillance follows the trail of outsourcing, as well as reproducing the network structure of contemporary capitalism. In the case of the US government, intelligence agencies no more wield surveillance directly. Contractors, such as the Booz Allen Hamilton company, are given the task to spy communications. Moreover, corporations, store the data of their customers and are ready to sell them to the US government in change of enjoying privileged conditions within the market. This pattern provides a more in depth, invasive surveillance, as well as boosting the shift to a more intelligence-led, predictive model of policing (James, cit.).

On the other hand, the development of communication networks, enables everyone to gain as many information as possible about individuals, firms, political groups as possible. In a rhizomatic society (Deleuze & Guattari, 1977), information does not circulate from the top to the bottom, but spread across society through

clusters of groups and individuals located in strategic places. By an in depth scrolling through the web one can access, gather and process a large amount of data, that span from individual biographies to the nature of corporations. Social networks, for example, can provide with those essential data that helps making up one's own mind about a person private life. In the same way, it is possible to know about corporations core business, partnerships, contracts.

In other words, the internet is two-faced, as it both increases the chances for control from economic and political power and the possibility to uncover and reveal them, as well as using the web and technology for alternative uses to those of capitalism. In Marxist terms, class struggle around the possession and control of the means of production also concerns the web. State power, platform capitalism, contractor, take the same side in the development of those control strategies that monitor the interactions on the web both to gather those data necessary to produce and circulate a new brand (Klein, 2001), to prevent the development of eccentric, alternative behaviours and practices, to control workers and marginal groups. Political activists take the side of the new working class that contemporary capitalism controls (Negri and Hardt, 1995; 2001; 2004) by colonizing its private sphere. As class struggle entails that society is divided between dominant and subjugated social groups, surveillance from below is strongly discouraged and criminalized by those who are vested with power. Outright repression practices, such as the control through spywares of the computers of alleged groups "at risk", is sided by the control of information. It becomes thus possible for the dominant social groups who either possess or control the web to circulate a hegemonic discourse (Gramsci, 1973) that depicts media and web activists as criminals and presents the internet as a sort of cybernetic heaven, where one can get access, through the mediation of money, to as many goods as possible. Assange and his *Wikileaks* partners have demonstrated that alternative uses of the internet are possible, as well as revealing classified news about relevant State and corporate crimes. They did it through the elaboration. and enactment of alternative practices, more threatening and articulated than the other forms of alternative surveillance that currently exist. The criminalization of Julian Assange and *Wikileaks* is part of the political struggle for the control of cyberspace. More than other forms of unconventional use of other forms of cyber-resistance, Assange and *Wikileaks* posed a threat to the dominating powers. That was the reason for their criminalization. The next section will analyze this aspect in depth, by focusing on the construction of the concept of cybercrimes. After arguing for the need to develop a critical view about it, the analysis of different forms of cyber-resistence, as well as of counter-surveillance, will be explained.

3.The *legitimate threshold* of cybercrimes: Assange as a *subversive cybercriminal*

Howard Becker (1963) has unraveled the dynamics underpinning the process of criminalization. Moral entrepreneurs moved by purposes of reform gain the political support of mainstream public opinion by using their possession of material, symbolic and relational resources. Such a power network (Ruggiero, 2016) mobilizes those actors involved in the production and enforcement of rules, such as politician, police forces and magistrates in the repression of alleged cybercriminals.

Since the use of IT, in particular the surfing on the Internet, have grown to be prominent in social relations, a widespread moral panic has taken over Western societies. Such crimes as cyber-bulling, revenge porn, paedo-pornography, frauds, identity thefts, have taken advantage of the opportunities the web provides, such as anonymity and fluidity. Whereas one cannot deny the existence of these crimes, as well as the danger they pose to the community, on the other hand there exist a gap between the real danger and the representation of the phenomenon. Some authors (Treadwell, 2012) show how cybercrimes are mostly committed by either individual actors or by temporary networks of persons who constantly move between the legal and the illegal space. Media and enforcers hardly take this analysis into consideration, as they indulge in the representation of the web as a dangerous virtual place, haunted by treacherous entities. The circulation of such a narrative serves two purposes: the first is that of fuelling the media industry and to provide a mass audience, out of which the creation of web thrives. Cyber marauders are the new threat for society, endangering our bank accounts and privacy.

Moreover, the narration about foreign cybercriminals, in particular Russian, poses a threat to democracy and freedom. IT experts hired by the Russian president, Vladimir Putin, are regularly held responsible for spying, circulating fake news, influencing democratic elections, thus fueling the xenophobic rhetoric around the enemy and the resentments against migrants and refugees. It is out of this multilayered panic that governments feel legitimized to implement such policies as the Project Carnivore or enforce worldwide spying devices like the Echelon project. Like in the case of street crimes, fear (Simon, 2007), provides political power with the necessary justification to widen the net of social control (Cohen, 1985), and to tighten it at the same time through the forging of new criminal behaviors and the implementation of new repressive measures.

Political powers reproduce the dialectic between inclusion and exclusion through the production, also in the cyberspace, of a space of exclusion of those unconventional behaviours, lifestyles and expectations that pose a threat again the dominating power relations. An outcome that can be reached through the use of that state of exception (Schmitt, 1993; Agamben, 2017) that, while widening power, restricts civil liberties and increases criminalization. The category of cybercrime becomes, by this token, a wide container wherein all the kinds of behavior on the web

can be included, ranging from media activism to cyber-bullying. Under this scheme, Julian Assange can be deemed as criminals, both because they use the web to commit crimes and because, as they have access to classified data, they are accused of endangering national security, as well as suspected to work for a foreign power.

The use of a different criminological point of view, like the one provided by Kevin Steinmetz (2022), can be helpful to debunk the issue of cybercrime, as well as to de-criminalize Julian Assange and *Wikileaks*. Moreover, it will help unmasking the conflicts around the use of the web. Moving from a realistic approach, Steinmetz argues that, in order to consider a behavior as criminal, it is necessary to assess whether it is harmful or not for the public, causing social harm within the community. Steinmetz propose a distinction between primary and secondary harms. The former are the economic, psychological and environmental crimes that are caused by cybercrime. The latter are those harms caused by surveillance, that is censorship and manipulation through the growing monopoly of the majors, as well as fueling punitive attitudes. Despite the distinction between primary and secondary is arguable, as zemiologists (Whyte et al., 2015) show that it is what Steinmetz defines as "secondary harms" to damage society more seriously, the point he raises is relevant insofar as it evidences that surveillance, performed either by the state or by private actors, is also a criminal behavior. This being the case, the definition of cybercrime is not so straightforward and objective as mainstream public opinion pretends it to be.

The definition of crime, as well as the criminalization of individuals and social groups, are the outcome of power struggle in the economic and political spheres. Assange and *Wikileaks* were criminalized under the dominant pattern of laws and opinions, shaped by the dominating social and political forces. Moreover, if one takes into consideration the aspect of social harm, it will be possible to argue that Julian Assange, Edward Snowden, Chelsea Manning and the *Wikileaks* activists, far from harming the public, engaged in a beneficial activity. This is because they produced and circulated alternative information to make public opinion aware of the atrocities committed both by governments and by corporations. A subversive activity, as it overturns the meaning of crime and allows to see power under an opposite point of view. What governments, media and corporation call "national security", "marketing" or "information" are indeed atrocities, spying activities and disinformation, that is they are *crimes of the powerful* (Ruggiero, 2018).

Such an overturning of political perspective cannot be tolerated and makes it necessary for power agencies to regain the lost ground by using labeling, criminalization and prosecution to make sure that such subversive practices as that enacted by Assange will not be followed. The treatment Assange and Manning experienced combines the repressive aspect with the deterrent one, because of its radical, innovative approach and structure. In the next session, these aspects will be focused upon.

4. To hide or to organize. The radical practice of *Wikileaks*

George Orwell, in his dystopian novel *1984* (1950), warned about the importance for power to control, manipulate and circulate information. Other authors, conversely (Negri, 1997), argue about the importance of sabotage, that is a pattern of articulated practices aimed at contrasting the capitalist domination while, at the same time, creating the condition for a new social organization, as well as e new mode of production.

In relation to the problems that relational surveillance poses, theories and practices of sabotage have developed following different paths. Geoffrey De Lagasnerie (2015), in his reflection about the practices of *Wikileaks*, reaches the conclusion that we are facing a structural change in public sphere. Since relational surveillance consists of an invasive control of the innermost individual spheres, and dominant media actors both produce and circulate disinformation, the new strategy of resistance should consist of hidden practices, carried out through secret identities. De Lagasnerie refers to the practices of Anonymous, which are successful insofar as unidentifiable individuals and groups enact them. Anonymity is even stronger if coupled with unpredictable acts, so as to take surveillants by surprise.

Whereas one can agree with De Lagasnerie about the impoverishment of public sphere, it is very unlikely that such alternative practices can be effective. Firstly, because anonymity means that people engaged in such activities cannot communicate between each other, so that their actions will remain on an individual range, that cannot be characterized as part of a collective project of alternative society. Secondly, because anonymity can make way for every kind of protesters, differently characterized, and often opposed to each other. A no global activist, a fundamentalist Muslim, an environmental militant, a neo-fascist or a MAGA member, could all use secrecy, anonymity and unpredictability as political practice, in the same moment, for the same purpose. The consequence of their actions will surely be the creation of new moral panic and provide the justification for the enforcement of restrictive and repressive "exceptional norms". Finally, in order to coordinate each other effort, to reach a shared purpose, to gain the consent of a large amount of people, it is necessary to discuss publicly, also to improve the theoretical and practical aspect of an alternative project.

Elizabeth A. Bradshaw (cit.), in her analysis of sous-veillance, emphasizes two positive aspects of this practice. The first one relates to its peculiarity of "surveillance from below", an aspect entailing two qualities: media-activists, as well as gathering and circulating documents about power abuses and brutalities, when practicing sous-veillance, also propose a different use of new digital technologies. Whereas the dominant, neo-liberal based, narration about IT stresses its value for consumerist purposes, such as shopping online, sous-veillants show the way to an

alternative use of technology as a tool of defense of civil liberties. The second positive aspect of sous-veillance relates to the organizational aspect. One cannot fight against power without an organization. This is why such agencies as Indymedia proved to be useful during the G8 of Genoa, in 2001, when it was possible to unmask the brutalities made by the Italian police (De Gregorio, 2002) against the no-global activists thanks to a two level work: direct action by photographers, reporters, video-makers, militants taking picture with mobile phones, could become public and circulate an alternative report on what had happened because of Indymedia, that worked as a collective subject coordinating all the documentation efforts that activists had done. Working publicly, in an organized way, by making an alternative use of the media, can pave the way for a reinforcement of public sphere.

When it comes down to change uneven power relation, though, sous-veillance is not "subversive" enough. Sous-veillants work in a defensive way, as they reveal and circulate the misdemanours committed by the powerful, so that one could imply that they still have faith in liberal-democracies and their report aims at re-establishing the principles of civil liberties that might have been undermined by such episodes as either police brutalities or unfair arrests.

Julian Assange, as some authors point out (Anderson, cit., p.10), pushed the boundaries of resistance forward, by drawing on the cypherpunk experience. His resistance practices combined direct action and organization with the use of specific tools, such as cryptography and the Tor browser. Such devices are, according to Anderson (cit., p.7-8) anti-imperialist and anti-colonial devices because their use allows to dodge the surveillance practices enacted by governments, in particular the US Anti-Terrorism Bill (1991), promoted by the then Senator Joe Biden. This bill prescribes the restriction of cryptography, and the obliges private firms to provide the government with the data about their customers.

Assange and his *Wikileaks* partners, though their cypherpunk-inspired practice, engage in anti-imperialist and anti-colonial activism that consists of subverting the dominant logic about transparency and privacy. Whereas governments claim the right to privacy for their deeds and pretend to be entitled to violate individual privacy for sake of security, Assange moves in the opposite direction. Since power relations are uneven, it is possible to have a democratic society only if the powerful are under public scrutiny and common citizens are granted their right to privacy. To advocate transparency for the deeds of government and corporation becomes more and more necessary in contemporary age, when climate change, sharp social inequalities, war atrocities, police brutalities, make the world a more and more uncomfortable place to live in. To unveil the dark side of power means to change the political balance. In other words, to subvert power relations, since dismantling secrecy means to weaken a power that, under the name of security and prosperity, has kept hidden from the public view many negative aspects: tortures, nuclear experiments, ecologic disasters, indiscriminate killings. Julian Assange,

consequently, has been criminalized, prosecuted, arrested and held under hard conditions of detention because of his attack against the most important touchstone of power, that is secret. A tool that governments use to justify their state of exception and private firms justify under the claim they need protection from competitors.

Following this path, one can agree that the subversion of Julian Assange is due to his articulated practice, which on the one hand unveil power plots and on the other paves the way for an alternative social pattern. This is only in part true, at least in relation to what happens in the sphere of public opinion. If we would like to extend the discussion to other aspects, for example to the relations of production that make up the contemporary capitalist society, probably the practice of Assange would not be enough to subvert class relation. Whereas his lesson about direct action, organization and the use of specific tools to fight class oppressors, it could be argued that probably, the weak spot of *Wikileaks* was that of not connecting with those social movements who fight economic inequalities and extractive capitalism (Mezzadra & Neilson, 2013).

On the one hand, one could argue that information, nowadays, is a crucial area of production of surplus value (Lazzarato, 2000), so that Assange's practices, as well as having an anti-imperialist and an anti-colonial stance, are also anti-capitalists. On the other hands, the advancement of globalization, the impoverishment of Africa countries caused by the measures imposed by such organizations as the World Bank and the International Monetary Fund, have reshaped capitalism in depth, causing the development of multi-faceted anti-capitalist movements.

A connection between new social movements and *Wikileaks* would help shaping a more compact and stronger fighting front, that, as well as avoiding the criminalization of dissent, could expose the crimes committed by the powerful as the only kind of crime and promote a widespread mobilization. I am aware that, in order to achieve this outcome, it is necessary a mutual will to walk in this direction. It is very important to evidence this aspect, because one of the reasons why Julian Assange could be labeled as a criminal, forced to hide and then kept under hard conditions of detention, is related to the underrating of his action by many anti-capitalist forces. Tradtional left parties, trade unions, as well as new generation activists, were quite shy in mobilizing themselves on behalf of Assange and *Wikileaks*, as they failed to recognize the cause of media activism as their own cause. A mistake that has caused Julian to suffer slandering and imprisonment, and the movements to suffer a progressive weakening. Because of a misunderstanding that could and should have been avoided. Let us hope is not too late.

Conclusions

There are many points one can make at the end of this work. The discussion I have tried to develop aimed at providing a critical point of view about IT, cybercrime, resistance and the perspective of an alternative political project. The first reflection concerns the apocalyptic view about technology, and the internet in particular. As both individual and social life tends more and more to be mediated by IT, there is no reason why we should be afraid of IT. It is not about passively accepting that we are living in a more and more technologized world, wherein the borders between the real space and the virtual space tend to be more and more blurred. Consequently, the demonization of IT is out of place, because every transformation brings about, along with dangers, also positive opportunities.

Secondly, the definition of cybercrime, like that of crime in the real space, is the product of social and political struggles. It is by this token necessary to debunk the rise of moral panic about cybercrime, by carrying out a massive deconstruction of all the narrations about it. In the case of Assange, sous-veillants, and hackers, the label of cybercriminals is a "political" one, as labellers are afraid of losing their privileges and power. The use of the web for the purpose of sabotage, as well as to unveil the atrocities and ambiguities of corporations and States, can be considered a practice of resistance and opposition. That is precisely what Julian Assange and *Wikileaks* put in practice. That is why they were criminalized. Their criminalization follows the usual pattern of labeling: on the one hand, the status of the accused is deteriorated, as Julian Assange was accused of "treason" by a country he is never been a citizen of. On the other hand, the alleged danger posed by the alleged traitor cybercriminals justify the enforcement and reinforcement of a state of exception-like measures, such as spying, censorship and manipulation.

Thirdly, Julian Assange and *Wikileaks* were criminalized because of their peculiar political practice. They combined the individual action direct and the revelation of classified information enacted by sous-veillance activists with counter-surveillance activities, by claiming that, in an uneven society, power relations can be balanced only by making power dynamic transparent and, at the same time, protecting the privacy of ordinary citizens. Their crime was therefore that of *subversion,* insofar as they subverted power relations.

Fourthly, the acts of subversion Assange and *Wikileaks* put in practice, despite the international solidarity they enjoyed and the innovative practice they designed, suffered from *isolation.* In other words, many social and political anti-capitalist movements did not consider the battles of Assange as *their* battles. This was due to a mutual misunderstanding, because on the one hand, many movements who prioritize anti-capitalism do not recognize the battle on the web as worth being fought, or they deem civil liberties as a minor issue in comparison to larger capitalist exploitations. On the other hands, Assange and *Wikileaks* were focused on information but hardly

made capitalist claims. A lack of communication that made criminalization and repression possible, and that resulted into the weakening of *Wikileaks*. A weakness we cannot afford in an age of forthcoming global wars. A coordination between the many anti-capitalist movement, able to bring about shared strategies and project, is strongly necessary in these times haunted by Donald Trump and Elon Musk, and by the use they make of the web.

Conflict of interest

The author declares that there is no conflict of interest.

REFERENCES

Agamben, G. 2017. *Homo Sacer. Il Potere e la Nuda Vita.* Rome: Quodlibet.

Anderson, P. 2022. Of Cypherpunks and Surveillance. *Surveillance and Society,* 20(1): 1-17.

Ash, A. 1993. *Post-fordism. A Reader.* London: Routledge.

Becker, H. 1963. *Outsiders.* Glencoe, NJ: Free Press.

Bradshaw, E. A. 2013. This is What a Police State Looks Like: Sousveillance, Direct Action and the Anti-corporate Globalization Movement. *Critical Criminology Journal,* 21(7). 447-461.

Cohen, S. 1985. *Visons of Social Control,* Trenton, NJ: Transaction.

De Gregorio, C. 2002. *Non Lavate Questo Sangue.* Milan: Mondadori.

De Lagasnerie, G. 2015. *L'Art de la révolte. Snowden, Assange, Manning*. Paris: Fayard.

Deleuze, G. and Guattari, F. 1977. *Anti-Edipo.* Turin: Einaudi.

Eco, U.1963. *Diario Minimo.* Milan: Bompiani.

Foucault, M. 2007. Sicurezza, Territorio, Popolazione. Milan: Feltrinelli.

Geer, D. 2016. *Cybercrime. Digital Cops in a Networked Environment*, New York City, NY: New York University Press.

Gramsci, A.1973. *Quaderni dal Carcere,* Rome: Editori Riuniti.

James, A. 2015. *Intelligence-Led Policing,* London: Routledge.

Klein, Naomi. 2001. *No-Logo.* Milan, Italy: Mondadori.

Lazzarato, M. 2000. *Capitalismo e Conoscenza.* Rome: Manifestolibri.

Lyon, D. 2016. *Surveillance after Snowden.* London: Polity Press.
Lyon, D. 2018. *The Culture of Surveillance.* London: Polity Press.

Maurizi, S. 2023. *Il Potere Segreto.* Rome: Chiarelettere.

Mezzadra, S., and Neilson, B. 2013. *Border as Method, or, the Multiplication of Labor*. Durham, NC: Duke University Press.

Negri, A. (1997) *I libri del Rogo,* Rome: Deriveapprodi.
Negri, A., and Hardt, M. 1995. *Il Lavoro di Dioniso.* Rome: Manifestolibri.
Negri, A., and Hardt, M. 2001. *Impero.* Milan: Rizzoli.
Negri, A., and Hardt, m. 2004. *Moltitudine.* Milan: Rizzoli.

Radcliffe, J. 2016. *Intelligence-Led Policing.* London: Radcliffe.

Ruggiero, V., and Montagna, N. 2007. *Social Movements.* London: Routledge.
Ruggiero, V. 2016. *Perché I Potenti Delinquono.* Milan: Feltrinelli.
Ruggiero, V. 2018. *I Crimini dell'Economia.* Milan: Feltrinelli.

Simon, J. 2007. *Il Governo della Paura.* Milan: Il Saggiatore.

Suvin, D. 2024. I am afraid of AI, https://www.historicalmaterialism.org/article/i-am-afraid-of-ai/, [accessed January 19, 2025].

Tien, L. 2016. Architectural regulation and the evolution of social norms. Daniel Geer (ed.). *Cybercrime: Digital cops in a networked environment*. 37–58. New York City, NY: New York University Press.

Treadwell, J. 2012. From the car boot to booting it up? eBay, online counterfeit crime and the transformation of the criminal marketplace. *Criminology and Criminal Justice*, (2)2. 175-191.

Vecchi, B. 2019. *Il Capitalismo delle Piattaforme.* Rome: Manifestolibri.

Vegh Weiss, V. 2021, ed. *The Criminalization of Dissent,* London: Routledge.

Ventura, H., Deflem, M., and J. M. Miller. 2005. Governmentality and the War On Terror: Fbi Project Carnivore and The Diffusion Of Disciplinary Power. *Critical Criminology Journal,* (5)13, 55-70.

Whyte, D. 2015, ed. *How Corrupt is Britain?* London: Pluto Press.

Zuboff, Shoshanna. 2019. *Surveillance Capitalism.* Washington, DC: Oxford University Press.