10
CYBER OUTSIDERS
Julian Assange and the labelling of online activists

Vincenzo Scalia

Introduction

The Australian media activist and journalist Julian Assange, one of the founders of the Wikileaks site, is a controversial figure of contemporary history (Maurizi, 2021). Assange was arrested on the 11th of April 2019 inside the Ecuadorian embassy he had been living in as a refugee since June 2012, after the president of the Latin American country deprived him of his refugee status. He was eventually detained in London's Belmarsh prison by the British government, as the United States government is seeking his extradition (Crouch, 2019). Washington claims (Global Freedom of Expression, 2023) that Assange is liable of a high treason accusation for putting USA security at risk. Such a charge would result in a 175-year jail sentence. On the other hand, among Western civil society, many have protested the arrest and extradition request (Melzer, 2023), contending that the prosecution of Julian Assange contradicts the most outstanding standpoints of Western democracies, such as freedom of speech and freedom of the press.

This chapter will use the case of Julian Assange as the starting point for a reflection about the web as a new space (Hayward, 2012) wherein the borders between legal and illegal, legitimate and illegitimate, licit and illicit behaviours are drawn. One can argue that the internet can be seen as a social framework wherein different groups and individuals, endowed with different interests, values and aims, engage in power-related conflicts. The outcome of such clashes is the division of society between the *insiders*, who set up the rules, and the *outsiders*, who are criminalized as they do not fit into the pattern of rules that has been set up (Becker, 1963). The web is a double-edged sword; on the one hand it can be seen as a tool allowing the free flow of interactions between its users, on the other hand it is a tool of social control by the most powerful social groups; that is, the corporations and the State, whose use of the web aims at shaping and controlling the choices of global consumers. This conflict results in the production and enactment by the outsiders of those practices that aim at challenging and overturning the dominating pattern of rules. One can define such practices as *counter-surveillance*, or the possibilities of controlling the controllers provided by the web. Julian Assange, like other web activists, has thus wielded a counter-power, as he has used the web both to get hold of secret information and to make

DOI: 10.4324/9781003277675-12

the public aware of the way governments works by circulating the material he found. The practice that Assange and his Wikileaks partners have enacted makes them outsiders, as it triggers the reaction of the states that suffered the hacking of their security sites. The problem is that those who react against Assange are the same social groups that set the security rules and, at the same time, committed those global crimes that whistleblowers have revealed (Ruggiero, 2016). Assange violated the rules of secrecy, but at the same time, he put into practice the freedom of speech (ACLU, 2023b). Moreover, if transparency is supposed to be one of the standpoints of democracy, its violation could help those who want to advocate the abolition of state secrets in the pursuit of their aim. In order for the public to assess the quality of its leaders, information about indiscriminate killings of civilians or about surveillance through the use of IT become crucial resources. This being the case, one could argue that Assange was *labeled* as a deviant and a criminal because of his opposition to the current political and economic *status quo* that set and enforced the rules of the web.

This chapter will use Assange as a starting point to discuss the definition of online deviance. The first part will analyse the ambiguities of the web under the penal aspect. It will be possible to see from the outset how the web follows some patterns of control produced and enforced by powerful groups (IT majors, entrepreneurs and the state) for sake of controlling web surfers and orienting their market choices. In the second part, an in-depth discussion on the Assange case will bring to the fore the issue of social control in connection with relational surveillance and its potential of resistance to power. The latter concept draws on the ideas of Michel Foucault (1980), who argues that in order to resist the dominating narrative of power, it is necessary both to elaborate on and to enact an alternative set of strategies that make room for an alternative pattern of values and interests.

The process of labelling will be analysed through a three-stage scheme I propose to adapt: *slandering*, referring to the attacks on the reputation of Julian Assange; *isolation*, which consists of political pressure on Assange's potential supporters; and finally, that of *repression*, concerning what follows the arrest. In all three stages it will be possible to see a combination of the State's repressive force with ideological elements, such as that of national security, or instrumentally using such issues as sexual violence, which eventually proved flawed. The definition of Assange's practice as *counter-surveillance* and his consequent labelling as deviant and a criminal by the social groups who hold power will be discussed in the third part. A conclusion will be dedicated to a reflection of the penal implications on the web: virtual space is like the social space, with deviance being a definition forged by those who hold the internet under their control. The real solution is that of pushing further for democratization and transparency.

The ambiguities of the net

The bursting affirmation of the IT-based network as the fulcrum of social relations has led some scholars to speak of the "third space": like the natural environment and society, we find ourselves in a context characterized by its own rules, by independent dynamics, by peculiar conflicts, by completely new representations and identities. In terms of crime, new opportunities would also be produced within the third space, ranging from online scams to child pornography, passing through the so-called "cyber-terrorism". In other words, the network, in addition to increasing and modifying relational possibilities, also has the effect of producing new moral panic, with new moral entrepreneurs ready to stir up the bugbear of new threats to be exorcised by implementing measures. The securitization of

the network is also felt on the political level. Since the third space is structured from the outset as a public space which accessible to everyone without relevant censorship, two types of political struggles are produced within it: the first concerns the use of the network to create and disseminate alternative political practices. Not surprisingly, many of the recent social movements, such as Occupy and the Arab Spring, have been born and spread online. The second concerns resistance and insubordination towards a power that also manifests itself in cybernetic forms, as in the case of whistleblowers who operate through the use of encrypted platforms or through the use of the deep web. The hackers, or Julian Assange and Edward Snowden, might be included within this typology of web surfers. Therefore, a deeper perspective on network security is created, where control strategies and moral panic intertwine directly with the prevention and repression of the emergence of alternative discourses and practices. To better understand the relation between alternative uses of the web and the repressive practices enacted by the stakeholders (majors, governments, platform owners), it is necessary to create a more in-depth analysis, in order to also consider crime-related issues.

How real is the cybercrime threat? Is the definition of *cybercriminals* a way of labelling whistleblowers? How is it distinguished from other types of crime? How is the dialectic between freedom and security articulated? Some authors (Gottschalk, 2010) respond by depicting the identity of the cybercriminal. They refer to an individual with specific skills, jealous of his criminal identity, using the network for his illicit purposes and a member of criminal networks. The existence of such a criminal threat would require the need to control and limit the use of the network. The creation of a cyber-police that uses the most sophisticated technology would serve this purpose well.

James Treadwell (2012), Goldsmith and Brewer (2015) are concerned with criticizing this approach by highlighting its limits. The first underlines how the network constitutes a real bazaar: it is possible to find the most varied actors operating in different fields. The Internet, Treadwell tells us, is characterized precisely by its fluidity: not only it is possible to adopt multiple identities, but one can choose to operate simultaneously within legal and illegal domains, thanks to the guarantee of anonymity. This also applies to illegal activities. On the internet, as in the social space, mostly minor crimes are committed, and the perpetrators, as shown by a study of some workers in the East End of London, are not habitual criminals, nor do they possess sophisticated skills (Treadwell, 2012, cit.). They carry out small-scale fraud when they are in economic difficulties, and intermittently as well as individually. The latter move along the same path as Treadwell, speaking of the existence of a real "digital drift". The network users pursue a multiplicity of behaviours, implemented in an unstructured way and often according to instrumental purposes. Consequently, the bonds that are created on the network denote a certain transience, which makes it difficult to talk about the existence of criminal networks.

These analytical approaches, although important, leave out two aspects of cybercrime that are crucial as they mirror the debate on crime that crosses the non-virtual public sphere: how much security must be guaranteed to users of the network? Who has to guarantee it? To what extent does security clash with civil liberties or justify the choice to classify some practices? The state, through its preventive and repressive apparatuses, comes back into play, staging the issues of social control and the relationship between freedom and security. These aspects denote direct political implications: in the second space the security discourse has catalysed the repression of dissent, and in the third, the cyber-criminal threat can become a blunt weapon to wield towards ever-wider types of non-compliant behaviour.

As Giorgio Agamben (2017) points out, drawing on the work of Carl Schmitt (1982), states thrive on the establishment of a pattern based on the friend-enemy dialectic; that is, translated into the criminological language proposed by Howard Becker (1963, cit.), the distinction between insiders and outsiders. Assange, Manning and Snowden are the *enemies* to be dealt with accordingly. The construction of what one could define as *cyber-enemies*, though, must be understood within the contradictions that arise inside the web.

State regulation of the network presents a qualitatively relevant problem, which Daniel Geer (2016) connects with the so-called "digital physics". Unlike the material space, the third space is characterized by its fluidity, volatility and unpredictability; these characteristics intersect with the protection of civil liberties and the free market. Consequently, individuals and economic actors are unwilling to provide vital information about their existence and their interests to the actors' social control, which would make it problematic to implement all kinds of security measures on the net.

In reality, according to Lee Tien (2016), the reading of the network as a free and uncontrolled flow of relations and information turns out on second glance to be limited, insofar as the network works according to the principle of regulation. As a house orients and determines our movements according to its conformation, so the network orients our digital paths, creating the conditions for an ex-ante control based on the pre-determination of cybernetic navigation. Unlike the physical-social environment, where sanctions are imposed ex-post, the computer limits and directs our drift into the digital space right from the start. We follow from the beginning the directories of the web, and we are immediately told not to use abusive or offensive language, images or footage.

It is within this pre-regulated framework that space is created for a new form of surveillance: horizontal, imperceptible, pervasive; in other words, as David Lyon (2007, 2009, 2016) defines it, it is relational. Surveillance refers to all those activities aimed both at preventing and repressing any formal or informal breach of the rules that keep the social fabric together. The activity of watching the way members of a society behave allows those actors vested with formal and legitimized power to intervene in order to suppress the risk of anomic drifts (Durkheim, 2000). Surveillance is strongly related to power relations as the dominating social groups, or the insiders, make and enforce the rules against the marginal social groups, or the outsiders (Becker, 1963). Surveillance can thus be defined as an activity aimed at reproducing the existing force relations and the uneven power distribution within the social spectrum.

There are two different kinds of surveillance (Wood & Monahan, 2019): the first is formal; that is, all those activities of control that are carried out by the state through its apparatuses by relying on legal entitlements (Weber, 1971): police, magistrates and the army wield formal social control to deploy a surveillance one can define as vertical due to its being wielded from the top, i.e., state power, to the bottom, i.e., society. Vertical surveillance requires a high degree of obedience, both to the rules and their enforcers. Whereas it is possible for the members of society to change those who make the rules to eventually indirectly change the rules, it is not possible to dodge formal rules, the violation of which entails sanctions from fining to imprisonment. Other authors (Cohen, 1985), depict a wider spectrum of formal surveillance by using the concept of social control (Cohen, 1985). This concept also encompasses those agencies whose aims are ostensibly those of support and care, as in the case of a welfare state. Here we also find relations of subjugation and domination, as individuals are required to adhere to the dominating system of values and aims.

Another form of surveillance is the informal one; that is, surveillance wielded by the group of peers, neighbours, family, religious groups and work colleagues, or the social capital in which individuals are embedded (Coleman, 1988). This is a horizontal kind of surveillance which usually requires individuals' cognitive adherence to the rules underpinning inter-individual interaction, although in this case it is also possible to formally abide by the rules while enacting a secret deviance. Michel Foucault (1980) defines both horizontal and vertical surveillance as disciplinary powers, as they both draw on social relations to produce a web of domination that is deployed across society. The aim of disciplinary power is producing docile bodies that comply with the discipline required by industrial society. On the trail of Foucault's reflections, Gilles Deleuze (1999) defines contemporary society as a society of control, mostly relying on a web of mutual surveillance to make sure that individuals comply with rules and expectations that are moulded and conveyed through the media. In Deleuze's view, society has assimilated control to the point of letting technology catalyse surveillance and report what happens to the agencies in charge of social control.

The social networks we frequent, the people we chat with, the sites we visit, can be monitored by digital control systems that make use of a wider-ranging security question to monitor both actors and communications considered "a risk". This is the case with the "Carnivore" project (Deflem & Ventura, 2005), a surveillance program prepared by the FBI and approved by the US Congress in the aftermath of September 11th. Law enforcement agencies can monitor, with the approval of the district attorney and for limited periods of time, those individuals and those portions of the network suspected of terrorism. The surveillance authorization can be renewed if the investigation reveals something that leads to believing that the suspicions are well-founded, which thus requires further investigation supplements. The Carnivore project has been severely contested by organizations active in the defense of civil rights (Deflem & Ventura, 2005, cit., p. 59), not only because it violates privacy and freedom of expression, but also because it is aimed above all at American citizens of Arab origin or of Muslim religion, leading to the a priori criminalization of entire sections of the population.

Alongside the Carnivore project, as Edward Snowden revealed in 2013, there are other network control programs developed and implemented by the National Security Agency, which are characterized by being much more sophisticated and articulated (Lyon, 2016, cit., p. 72). The internal security agency is in fact characterized as the main actor of relational surveillance, whose control programs do not only concern alleged Muslim terrorists but affect the entire population. The network surveillance work therefore aims to monitor every form of communication, relationship and practice that goes against the regulation architecture, and it monitors the activities of alternative groups and networks. In this context, figures like Snowden and Assange are dangerous, as they not only reveal the details of the current interweaving of power but also demonstrate the possibility of overturning the security flow through using the network in the opposite direction to the conventional one, which wants to create a docile, controllable and tameable user. Relational surveillance brings about the possibility of counter-surveillance in the use of tools of control provided by the web to produce and enact practices of resistance against power. This kind of practice consists of the detection, as well as of the revelation, of the crimes committed by *the powerful*, such as white-collar crimes and state crimes (Green & Ward, 2006) and of the social harm they cause (Whyte et al., 2015). As a consequence, the practices enacted by Julian Assange and WikiLeaks can be defined as counter-surveillance. They are an opposition not only to the existing power relations but also to the practices of control implemented both

by political actors, such as the state, and by economic actors like contractors, private companies, and the IT majors through the manipulation of Big Data (Lyon, 2019). Assange, with the help of Edward Snowden and Chelsea Manning, enacted a counter-manipulation as he accessed the Big Data provided by the governments and made them public.

In other words, there is no difference between the social space and the cyberspace: in both cases, the definition of what is legal and what is not is the outcome of a conflict with the state embodying the interests of the insiders and enforcing the law against the outsiders (Poulantzas, 1977). The state, at the same time, holds back from prosecuting more serious crimes, as well as itself committing some peculiar crimes related to prevention, to repression or to war crimes.

As in the material space, the moral panic around some small-scale crimes provides the right to implementation of repressive measures that pass through the criminalization of specific sectors of society. In the network the alarm for cybercrimes, amplified by the fear of terrorism, becomes the Trojan horse for repressive action and for the implementation of new forms of social control, as well as for the repression of new forms of dissent. On the other hand, it is the very fluidity of the web that allows the production and dissemination of dissenting knowledge and practices, both through individual actions, such as those of Snowden, and through the creation of more structured experiences, such as Wikileaks. This flow of social relations in the web is deemed dangerous by the rule makers, whose legitimacy could be put at risk by the revelation of misdeeds that contradict the official impartiality and neutrality of the state conveyed by all the official narrations.

The making of a villain: slandering, isolation and repression. Assange as *homo sacer*

The criminalization of Julian Assange, as well as of those media activists who revealed state secrets via the web, marks an unprecedented event in contemporary history: in 1971, the *New York Times* got hold of and eventually published the Pentagon Papers about the Vietnam War, revealing the US Army's raids against North Vietnam and exposing the White House to further stigmatization that increased the anti-war movement (Sheehan, 1971). Three years later, the *Washington Post* made the public aware of Richard Nixon's administrative misdeed in the Watergate case (Bernstein & Woodward, 1972). These cases, like the Abu Ghraib abuses scandal of 2004 (Greenberg & Dreitel, 2005), were made public and widely discussed without provoking any reaction by the United States government under the assumption that both freedom of the press and freedom of speech, two standpoints of Western democracy, provided the rights to publicize unknown state practices. The case of Julian Assange has seen a different approach, based on the criminalization and prosecution of the Australian media activist. It is this crucial to analyse this difference from a criminological point of view, as it poses the question: "Why is Julian Assange criminalized, unlike his colleagues of the past?" In following Howard Becker's labelling theory, this case fits into the concept of *social reaction* (Becker, 1960, pp. 803–810). Becker argues that crime is not an objective phenomenon. An act is deemed criminal when it is defined as such by those who make the rules (*insiders*). Secondly, the definition of crime would be ineffective without a social reaction to behaviour that is defined as criminal. For example, if the use of marijuana is illegal, a police officer seeing a group of people smoking dope in the park can choose either to sanction them or to just warn them that such a practice is not legal and force them out of the park. In following this pattern, one can follow an articulation of

the criminalization process in three stages: firstly, there is no such thing as a set of social phenomena one can define as *crimes*; as a consequence of this, the definition of either an event or a behavior as criminal is the consequence of the reaction, either by society or by institutional agencies; thirdly, criminals are drawn from the ranks of those groups outside of mainstream society; that is, the *outsiders*. In the case of Julian Assange, all these conditions are fulfilled.

Assange's activism was immediately portrayed as a crime by the American government after the release by Wikileaks, on the 5th of April 2010 (Maurizi, 2021, p. 35), of the video showing the killing of civilians in Iraq, dating back to three years before. The video had been provided by a US soldier in Iraq, Bradley Manning, who was later to be sentenced and to become Chelsea Manning after her decision to change sex. Its worldwide circulation through the web left public opinion puzzled, as it damaged the reputation of the USA government. The Obama administration overreacted to that, claiming that by circulating the video, Wikileaks had put the security of the USA at risk. Assange was charged with high treason under the Espionage Act the federal government had enacted in 1935. Assange consequently ceased to be a media activist and a journalist to become a criminal.

Such an overreaction is the consequence of the massive defamation the American government had been facing since the early 2000s, when the second Gulf War left Western public opinion perplexed because of the flaky evidence that Iraq's dictator, Saddam Hussein, had weapons of mass destruction. Moreover, the news of the serious violations of human rights in the prisons at Guantanamo and Abu Ghraib (www.aclu.org) had made things worse for the American government. Wikileaks had also circulated documents that proved the brutalities.

The two more important reasons for the criminalization of Julian Assange, though, might be related to the means Wikileaks used and to the nature of the organization itself. To the first point, Wikileaks had used the web both to get the material from Chelsea Manning and to circulate it. Unlike the *New York Times* and the *Washington Post*, who had relied upon "deep throats" providing them with restricted information, Assange and Wikileaks had made extensive use of the web in a subjective way: their use of the Tor software to dodge the online control and get hold of material due to their connection with hackers, as well as the use of the web to spread the information faster, contradicted the architectural regulation of the web. Assange has taken seriously the potential of the web as a free space, thus trespassing the paths for its use set up both by the software producers and by its institutional users: the market and the state. As a consequence, Assange is an *outsider*, as he follows a different set of rules and his idea of the use of the web is different than the prevailing one. His project, and that of Wikileaks, is not that of controlling the web surfers and orienting their market choice. Assange uses the web with the purpose of informing worldwide public opinion by making use of the potentiality of cybernetics, including the involvement of hackers, communication through encrypted software such as Tor and the circulation of classified material (Melzer, 2023, cit.). The purpose of Wikipedia is radically different from that of the USA government, but the latter are in the position of setting and enforcing the rules.

The labelling process, though, cannot happen without those *rituals of degradation* (Garfinkel, 1956) that deprive a person of their own identity and reputation to be stigmatized by the others (Goffman, 1963). This is what we call the first stage of Assange's labelling, which is *slandering*. The strategy of degradation consists of a false accusation of a serious crime that causes the rise of moral panic and triggers moral repulsion against a person. Such an accusation will prove successful to persuade the reluctant part of the public that the stigmatized

person is a villain rather than a person entitled to their rights. For Julian Assange, slandering meant the accusation of sexual violence. That accusation, dating back to late 2010 when Assange was in Sweden, was later to be dropped by the Swedish magistrates (*www.theguardian.com/media/2017/may/19/swedish-prosecutors-drop-julian-assange-investigation*). After Assange's arrest in London in 2019, the British prosecutor took the same decision.

Although the charges were eventually dropped (in 2017), the shadow of such a serious accusation hung for 9 years over the spokesman of Wikileaks, paving the way for the second stage of his labelling: *isolation*. This stage recalls the *secondary deviance* Lemert (1951) refers to and Becker has drawn upon. Whereas *primary deviance* relates to the deviant act, the secondary stage relates to the reaction society and enforcement agencies enact once an individual (or a group) has been labeled as deviant. The stigmatization of deviants means their marginalization from mainstream society. Their behaviour will be stigmatized to draw a line between them and the society of insiders. Assange was indeed denied the possibility to move freely across the world: the US government issued an extradition warrant for high treason, along with the Swedish government's international warrant for the accusations of sexual violence. Two of the most important Western states made Julian Assange a wanted criminal, with the Swedish warrant striking a blow against his reputation as an activist. Sweden has had a long tradition of human rights-oriented policies and has been known for decades as one of the most attentive states to women's rights. A warrant issued by Sweden for sex-related crimes, for a media-activist claiming to campaign for human rights, is more effective at marring the reputation than an American warrant (Maurizi, 2021, cit., p. 87). Whereas the latter is questionable as the border between high treason and freedom of press blurs, the Swedish warrant, as well as reducing Assange's movements across the Western world, casts doubt about his credibility as an activist, thus weakening both his campaigns and arguments he was the victim of an unjustified prosecution. The only chance he had was to seek refuge inside the Ecuadorian embassy in London, after applying for political asylum in the Latin American country on the 19th of June 2012. As Rafael Correa, president of Ecuador from 2007 to 2017, was sympathetic to Wikileaks' cause, Assange could live in the Ecuadorian embassy, although it was difficult for him to leave the premises because of the risk of being arrested (*www.washingtontimes.com/news/2012/aug/16/uk-we-wont-allow-julian-assange-to-leave-britain/*). As Western countries aligned themselves to the Swedish and American desiderata, Assange was spied on (Maurizi, cit., p. 130–164), with bugs and cameras being illegally installed inside the embassy. After Correa left the presidency, it was possible for British intelligence to infiltrate some agents under cover inside the embassy until Assange's asylum was revoked in 2019, thus making it possible to arrest him on the 12th of April. The isolation and arrest of Julian Assange makes the argument about labelling even stronger. While Assange was banned from travelling and forced to seek refuge in an embassy, living for seven years like a prisoner, the state crimes (Kauzlarich, 2001) committed by the British government, in the violation of Assange's privacy and the violation of Ecuador's embassy sovereignty until 2017, are not considered as the insiders, in this case the British government, makes the rules by and for itself (Ruggiero, 2016) and works out self-acquittal strategies based either on outright or on interpretive denial (Cohen, 2006). Such an uneven power relation produces an insider/outsider dichotomy, which turned out to be disadvantageous for Assange, who then faced the stage of *repression*.

Julian Assange has been jailed since the 19th of April 2022. The charges of sexual violence were dropped, but he is awaiting the final verdict about his extradition to the USA.

While the legal battle outside is raging as the extradition warrant was signed on the 16th of June by the British Home Minister Priti Patel (www.theguardian.com/media/2022/jun/17/julian-assange-extradition-to-us-approved-by-priti-patel), his solicitors have appealed the decision, both to the British Supreme Court and to the European Court of Human Rights, claiming that Assange is detained under inhumane conditions (*www.ecchr.eu/en/publication/the-detention-of-julian-assange-is-inhumane/*). The Belmarsh prison, where Assange is being held, is a Category A prison, hosting people convicted or accused of having committed serious crimes, such as sex offenders, terrorists and murderers. The British prison Ombudsman (*www.justiceinspectorates.gov.uk/hmiprisons/inspections/?location=belmarsh*) has several times in his yearly reports addressed the poor living conditions in the prison, indicating the repeated and disproportionate use of force by the prison staff. Julian Assange suffered from the harsh conditions of detention in Belmarsh, and a stroke hit him in December 2021. Moreover, his pathologies are against a prolonged state of detention under harsh conditions. Apart from the inhumane life conditions inside prison, Assange has yet to be tried for the alleged accusation by the US government. Moreover, he does not have a criminal record for crimes like terrorism or homicide. While he is awaiting extradition, the reason why he is being kept under such conditions needs to be reflected upon.

Assange is being accused of putting the USA's security at risk for circulating classified materials about the war. While public opinion worldwide could appreciate that it is hard to detect a relation between the documents circulated through Wikileaks and the security of the USA, Assange's responsibility does need to be ascertained in a trial that grants him the possibility of defending himself under habeas corpus and the Bill of Rights. Assange has indeed served a long pre-trial detention of three years and a half as this chapter is being drafted. Moreover, the state of detention is impacting his health. It appears the stage of repression articulates in two stages: that of the pre-trial detention Assange is currently experiencing, and the stage after he will be sentenced to jail by the US courts if extradited.

The US reaction looks more like a reprisal than a reaction against a violation of state secrets. There are indeed more complex dynamics behind it. Firstly, the issue of uneven power relations between insiders and outsiders is at stake. The US government calls a violation of security what a consistent portion of worldwide public opinion calls freedom of the press and of speech. There is no objective or a shared definition of freedom and crime. The borders between are legitimate. Thanks to the help of those *moral entrepreneurs* Becker refers to as agencies mobilizing public opinion about an issue (1963, cit.), the labelling process proves successful. Assange is labelled a villain by the US government. This label is accepted by the British government, which detains him under inhumane conditions and has agreed to his extradition (Melzer, 2023, cit., p. 143).

Secondly, labelling implies that the attention of public opinion is deflected from the heinous crimes that were committed during the Gulf War. It's likely, as the Chilcot report of 2017 demonstrated definitively that Tony Blair and his government deceived British public opinion to declare war on Iraq (*www.gov.uk/government/publications/the-report-of-the-iraq-inquiry*), that the British government is pursuing the same aim. A scapegoat, an enemy or a case to be put in front of public opinion will give governments the possibility of hiding evidence and crafting new justifications for what they did.

Thirdly, this paves the way for the self-acquittal of states. Their control of the bureaucratic machines, their legislation, their network of relations (Ruggiero, 2016, cit.) allow them to call an International Governmental Crime (Kauzlarich, 1995), or crimes committed outside a state jurisdiction by violating international laws, an act committed for sake of

AuQ2

national security. The exercise of fundamental rights will thus become a crime for the state's parameters, whereas the social harm (Whyte et al., 2015) caused by a war, the indiscriminate killing of civilians, the environmental disasters and other violations of human rights will be denied or hidden.

Fourthly, there is an outright conflict in the definition of acts and behaviors, as well as the enforcement of rules. This is because what is at stake is the control of a new space, the web, to be structured as a public space. Whereas the states and the majors pursue their aim of architectural regulation to force the surfers into pre-order paths, interests, aims and values, Assange and Wikileaks advocate an open, plural, complex and public access and use of the web, attempting to make the web the new arena of civil liberties. Their activities are by this token a danger for those who are in control of the web, particularly the states. This is because Assange and Wikileaks propose a different approach of resistance, one that does not imply the use of political violence (Ruggiero, 2006).

The relational quality of IT-based surveillance provides new potentialities to fight and counterbalance the control and subjugation attempts that surveillance capitalism conveys. Both on a micro and on a macro level, it is possible to enact and develop a plurality of strategies for counter-surveillance, or those practices that both individuals and groups implement to protect their liberties by controlling the controller. On a micro level, counter-surveillance is a widespread practice that all of us are involved in daily. To check a Facebook page or a university site in order to gather information about someone we know is an act of counter-surveillance, as it enables us to know many things we need about a person: residence, where they are at a certain time, lifestyle, political ideas, sexual orientations and so on. All this information is provided spontaneously by the users, who often neglect the issue of privacy and security. In any case, they make it possible for anyone with a basic knowledge of IT to easily acquire a significant amount of information about as many people as possible. On a macro level, it is necessary to possess more sophisticated skills, such as the use of more advanced search engines (like Tor) or the know-how to hack and crack the websites of governmental agencies and corporations. Another requirement is that of a network, both among hackers and crackers and those who work within the surveillance network and can leak classified news. The case of Julian Assange and Wikileaks matches all these requirements; firstly, because of the use of Tor, which allows for developing an underground connection between the sources and the members of Wikileaks. Secondly, Assange and his group possess those skills that enable them to hack the IT systems containing the information to be made public. Finally, the cases of Chelsea Manning and Edward Snowden demonstrate the importance of a network of infiltrators inside the surveillance apparatus; Manning was a soldier and Edward Snowden worked for Booz Allen Hamilton, one of the sub-contractors spying on the public on behalf of the American government. It was thanks to this articulated organization that Wikileaks was able to obtain the news about state crimes and circulate the information among the public. In other words, Assange and his partners exploited the potentialities of relational surveillance at its best. As watchful and disrespectful of civil liberties as surveillance can be, its contradictions allow those being surveyed the possibility of resisting and counteracting such surveillance, both by creating an alternative network to that of the dominating political and economic power, and by using the information acquired through this network to reveal the abuses committed by the dominating rulers against the public, thus enforcing a real democracy. Finally, as a consequence of this, the current rule-makers have been floundering, as they are facing an unprecedented challenge with new means and new contents. Such a vacillating power tries to restore its

foundation based on the *homo sacer* (Agamben, 2017), or the right to rule over life and death that power is founded upon. The border between outsiders and insiders, good citizens and villains, makes up a structural aspect of every society. When the border blurs it is necessary to reaffirm it in a radical way, by creating an enemy and punishing him (in this case) for the alleged danger he is accused of having created. In the case of Julian Assange, the friend/enemy, insider/outsider appears to have worked successfully. Consequently, the possibility and the practice of an open, free, plural web have been turned into crimes to be prosecuted with the harshest measures possible, such as confinement in a maximum-security prison and the threat of 175 years of jail for Assange, whereas Edward Snowden lives in Russia. Punishment and repression appear to be the answers that states provide to those who put fundamental liberties into practice. Julian Assange has not killed, injured or harmed anybody. He is accused of robbing or stealing information but, more than this, of publicizing it. One could argue we are facing a new kind of crime that has much to do with the virtual nature of the web. Fraud, identity thefts, forgeries and industrial espionage are being committed on the web. Assange did not commit any of these crimes. He obtained classified materials, but he did not do so for sake of making a profit or to advantage one market competitor against another. His criminalization and imprisonment appear to have slowed the activities of whistleblowers, as there is no notice of either new state crimes or of crimes of the powerful being leaked to public opinion. As illegal as his way of acquiring information might appear, it has much to do with the tricks of the trade, as journalists very often get hold of information (and use it) in ways that do not follow standard procedure. The trade-off between acquisition of material and publication has been positive up to now, as the interest of the public has been accomplished. In the case of Assange, the question is not *how to punish*, but *why punish?* The answer is because the Australian media-activist has committed a deviant act where the US government, in order to criminalize it, retrieved a law dating back to 1937. Moreover, Assange has followed the principles outlined by the freedom of information. More than this, he is not the first journalist or press-activist to do so. This important part of the labelling theory, that of enforcing a different kind of punishment, must be discussed under a different light. Following Becker's arguments on the use of marijuana (1953), which focuses on the connection between the drug and the social group that makes use of it, in his words African American jazz musicians, it is possible to argue that *decriminalization*, rather than *diversion*, should be the path to be followed in the case of Julian Assange and other media activists. Freedom of speech and freedom of the press are two standpoints of the social space. It is time to extend them to the virtual space.

Conclusions

The story of Julian Assange seems to give a negative answer to our initial question, as it looks like any attempt to make classified news public ends up being criminalized.

Some authors (Delagasnerie, 2020) have argued that the activism of Wikileaks proves that the only possibility of resisting power nowadays lies in the deployment of a strategy based on underground resistance. As surveillance is very invasive, activists must carry out their sabotaging of power by keeping and developing secret identities and activities. We believe this is not the case for Wikileaks for two reasons: firstly, because Assange and all his partners have always made public what they were doing and why. In the second case, their activity consists precisely of revealing to the public what the power conceals, thus reaffirming the value of public discourse against the arcana imperii, or the idea that a state's

security relies on the performance of secret activities by those vested with power. Norberto Bobbio (1987, cit., p. 63) argued that the security of power relies on the insecurity of citizens. Assange and Wikileaks have endorsed Bobbio's theorization by overthrowing it: the more insecure power is, the more citizens feel secure: Tony Blair's lies about the Gulf War, Guantanamo, Abu Ghraib, the bombing of Iraq and Afghanistan, as well as the news about financial and environmental crimes leaked by Wikileaks, reveal the real aspects of power, and at the same time show its weak spots, by empowering the public with the resource of information. Moreover, Wikileaks and Assange suggest making a fluid, democratic and open use of the web, unlike some other attempts, such as the Rousseau platform adopted by the Italian populist 5 Star Movement (Stockman & Scalia, 2020) to use the web to produce a plebiscitarian form of politics. The issue of privacy and freedom of speech, both in an active way (use of the web by the internet surfers) and in a passive way (protection of privacy from manipulation and surveillance) has been recently at stake once again, as Twitter/X was taken over by Elon Musk (Gallagher, 2022).

The American government considers Assange, Manning and Snowden as criminals because they revealed state secrets in violation of the web. While we appreciate that Julian Assange and his partners might not have respected the law completely, they did not behave any differently from those governments that had been spying on private individuals and sold information to private operators without obtaining consent. Finally, the real crimes, as many human rights organizations and civil society groups have pointed out, are those committed in Guantanamo, in Abu Ghraib and in the rendition protests (ACLU, 2023a). Such crimes need someone to push the boundaries of legality to reinforce civil liberties and democracy. Julian Assange and Wikileaks are the ones who have done this.

References

Agamben, G. (2017). *Homo sacer*. Quodlibet.
Becker, H. (1953). Becoming a Marijuana user. *The American Journal of Sociology*, *69*, 235–242.
Becker, H. (1960). Normative reaction to normlessness. *American Sociological Review*, *25*, 803–810.
Becker, H. (1963). *Outsiders*. Free Press.
Bobbio, N. (1987). *The future of democracy. A defence of the rules of the game* (R. Griffin, Trans.). University of Minnesota Press. (Original work published 1984). Retrieved from https://archive.org/details/futureofdemocrac00bobb.
Cohen, S. (1985). *Visions of social control*. Transaction.
Cohen, S. (2006). *Stati di negazione*. Carocci.
Coleman, J. (1988). Social capital in the creation of human capital. *American Journal of Sociology*, *94* (Supplement: Organizations and Institutions: Sociological and Economic Approaches to the Analysis of Social Structure, 95—S120). Retrieved from www.jstor.org/stable/2780243.
Deflem, M., & Ventura, H. (2005). Governmentality and the war on terror: FBI project carnivore and the diffusion of disciplinary power. *Critical Criminology*, *13*, 55–70.
Delagasnerie, G. (2020). *L'Arte della Rivolta*. Stampa Alternativa.
Deleuze, G. (1999). *Principio Metamorfosi. Verso un'antropologia dell'artificiale*. Mimesis.
Durkheim, E. (2000). *La Divisione del Lavoro Sociale*. Edizioni di Comunità.
Foucault, M. (1980). *Power/knowledge*. Harvester Wheatsheaf.
Garfinkel, H. (1956). Condition of successful degradation ceremonies. *American Journal of Sociology*, *61*(5), 420–424.
Geer, D. (2016). *Cybercrime. Digital cops in a networked environment*. New York University Press.
Goffman, E. (1963). *Stigma: Notes on the management of spoiled identity*. Prentice Hall.
Goldsmith, A., & Brewer, R. (2015). Digital drift and the criminal interaction order. *Theoretical Criminology*, *19*(1), 112–130.
Gottschalk, P. (2010). *Policing cybercrime*. Boon Boon.

Green, P., & Ward, T. (2006). *State crimes*. Pluto Press.
Greenberg, K., & Dreitel, J. (Eds). (2005). *The torture papers. The road to Abu Ghraib*. Cambridge University Press.
Hayward, K. J. (2012). Five spaces of cultural criminology. *British Journal of Criminology, 53*(3), 441–462.
Kauzlarich, D. (2001). Towards a victimology of state crime. *Critical Criminology*, *10*, 173–194.
Lemert, E. (1951). *Social pathology. A systematic approach to the theory of sociopathic behavior*. McGraw-Hill.
Lyon, D. (2007). *Massima Sicurezza*. Raffaello Cortina.
Lyon, D. (2009). *Oltre il Panopticon*. Raffaello Cortina.
Lyon, D. (2016). *Surveillance after Snowden*. Wiley.
Lyon, D. (2019). *The culture of surveillance*. Polity.
Maurizi, S. (2021). *Il Potere Segreto*. Chiarelettere.
Melzer, N. (2023). *The trial of Julian Assange*. London.
Poulantzas, N. (1977). *Il potere nella società contemporanea*. Editori Riuniti.
Ruggiero, V. (2006). *La Violenza Politica*. Laterza.
Ruggiero, V. (2016). *Perché i Potenti Delinquono*. Feltrinelli.
Schmitt, C. (1982). *Le categorie del politico*. Il Mulino.
Stockman, C., & Scalia, V. (2020). Democracy and the five stars movement. *European Politics and Society*, *21*(5), 603–617.
Tien, L. (2016). Architectural regulation and the evolution of social norms. In D. Geer (Ed.), *Cybercrime: Digital cops in a networked environment* (pp. 37–58). 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*, 175–191.
Weber, M. (1971). *Il Lavoro Intellettuale come Professione*. Einaudi.
Whyte, S. (Ed.). (2015). *Why is Britain corrupt?* Pluto Press.
Wood, M., & Monahan, T. (2019). Platform surveillance. *Surveillance and Society*, *17*(1–2), 1–6.

Websites

American Civil Liberties Union. (2023a). *Guantanamo bay detention camp*. Retrieved from www.aclu.org/issues/national-security/detention/guantanamo-bay-detention-camp
American Civil Liberties Union. (2023b). *Letter urging DOJ to Drop the charges against Julian Assange*. Retrieved from www.aclu.org/documents/letter-urging-doj-drop-charges-against-julian-assange (accessed 12 August 2023).
Bernstein, C., & Woodward, B. (1972, August 1). *Bug supsect got campaign funds*. Retrieved from www.washingtonpost.com/wp-srv/national/longterm/watergate/articles/080172-1.htm
Crouch, D. (2019, April 11). *Julian Assange faces US extradition after arrest at Ecuadorian embassy*. Retrieved from www.theguardian.com/uk-news/2019/apr/11/julian-assange-arrested-at-ecuadorian-embassy-wikileaks.
Gallagher, R. (2022, December 2). *Twitter firings gutted its compliance teams. Now it risks investigations and big fines*. Retrieved from www.latimes.com/business/story/2022-12-02/twitter-shrunk-compliance-teams-risks-investigations-fines
Global Freedom of Expression. (2023). *USA vs. Assange*. Retrieved from https://globalfreedomofexpression.columbia.edu/cases/the-government-of-us-of-america-v-assange/ (accessed 12 August 2023).
Sheehan, N. (1971, June 13). *Vietnam archives. Pentagon study traces 3 decdes of growing U.S. Involvement*. Retrieved from www.nytimes.com/1971/06/13/archives/vietnam-archive-pentagon-study-traces-3-decades-of-growing-u-s.html