Ethical and legal limits to the diffusion of self-produced autonomous weapons

Ethical and Legal Limits to the Diffusion of Self-Produced Autonomous Weapons

Elena Falletti[1] and Chiara Gallese[1,2,3]
[1]Carlo Cattaneo University, Varese, Italy
[2]University of Trieste, Trieste, Italy
[3]Eindhoven University of Technology, Eindhoven, The Netherlands
efalletti@liuc.it
cgallese@liuc.it

Abstract: The theme of self-produced weapons intertwines diversified ideas of an ethical, legal, engineering and data science nature. The critical starting point concerns the use of 3D printing for the self-production of weapons: the doctrinal and ethical discussion is open, while from a case-law point of view no published decisions have been found. From a technical point of view it should be noted that, being produced with materials other than metal, the weapons in question would increase their danger, since it would not be possible to ascertain their possession through metal detectors. This possibility demonstrates how the combination of the application of 3D printing and AI can lead to further development of Autonomous Weapon Systems, especially drones, which are no longer confined to science fiction novels, but may appear on the market for goods and even become available for mass consumption, and it stresses the need for the promotion of negotiations for the drafting of an international treaty banning the production and use of lethal autonomous weapons. The combination of such printers with biometric facial recognition algorithms raises concerns for the increasing issues of physical, individual and collective safety that may arise. In fact, the biometric recognition technology allows the identification of individuals through the measurement and analysis of the somatic or behavioural traits; it is based on intelligent software, modelled on the human ability to recognize and identify faces by collecting and analysing huge amounts of data, and it is able to evolve its skills beyond its programmer's initial intention. It is clear that allowing self-production of such devices by non-expert users could produce more damages than benefits. The purpose of this contribution is to study how to regulate the effects of such self-made autonomous robots, since their use may have a devastating and disruptive effect on public integrity and social peace, especially in case of violent riots.

Keywords: 3D printing, artificial intelligence, AWS, LAWS, autonomous weapons, biometric recognition

1. Introduction

The 'DiDIY' (an acronym for 'Digital Do-It-Yourself', digital craftsmanship) is a socio-technological phenomenon arising from the wide availability of digital tools, which facilitate the convergence of both physical and informational components as well as the increasing accessibility of knowledge and data through open online communities. This entails the emergence of new scenarios in the relationships between individual, organisational and social roles in which the distinction between producers and consumers/users blurs along with the approach of new challenges and opportunities. In fact, for some years now, the printing of three-dimensional objects has been talked about as a technological innovation capable of revolutionising manufacturing.

One of the first interesting models applicable to DiDIY could be Open Source Hardware, for example the well-known Arduino, or the Open Source Software, Free Cultural Works, or Creative Commons projects where the creators of knowledge release the use of their creations under conditions that can generally be summarised as follows:

- a) freedom of use for any purpose (within the meaning of the law);
- b) freedom to adapt other people's knowledge products according to their needs;
- c) freedom to copy and share with others;
- d) freedom to distribute modified versions.

If using 3D printers in manufacturing environment seems to open up new opportunities, there is actually one domain where this new scenario presents serious issues. This refers to the spread of 'ghost weapons', i.e. weapons moulded with 3D printing, which cannot be detected by metal detectors, and to the risks posed by self-made autonomous weapons (AWS).

This article analyses the legal issues concerning self-printed weapons, in particular AWS equipped with biometric identification technologies. The first part of the article will discuss the legal case of 3D-printed guns and

the publishing of their blueprints online. The second part explores the international regulation regarding autonomous weapons. The third part describes the legal implications of biometric identification technology, while the fourth part analyses the ethical implications of the use of AWS. Finally, the last part proposes a possible solution to address the risks generated by self-built AWS.

2. Build your gun! A US tentative to disseminate a manual for 3D self-printed guns

3D printing also presents ethical problems, e.g., in relation to the 'in-house' production of organs, tissues for transplantation, cells, and even drugs. On these points, the doctrinal and ethical debate is open and heated in the United States regarding the possibility of producing weapons of various calibre or size (Pasquale, 2020). In fact, the circumstance is already quite well known, and made headlines in 2013 when, after producing his own weapon, Cody Wilson published online a manual with instructions on how to make it with a 3D printer (Huang, 2022). As a result of the speed of the spread of this pamphlet and the dangerousness of its contents, its dissemination was banned by blacking out the site that hosted it, as such dissemination would be contrary to the Treaty on the International Traffic in Arms.

From a technical point of view, however, it should be noted that being produced with plastic materials processed with 3D printers, the weapons in question would increase their dangerousness since it would not be possible to ascertain their possession through the usual metal detectors. Indeed, the point about the material used to make the gun is really important, since according to federal law, it is legal to make your own gun, as long as it is within certain limits set by federal regulations (Huang, 2022). These latter are the International Security Assistance and Arms Export Control Act of 1976, as well as its enacting regulatory regime, the International Traffic in Arms Regulations (ITAR)[1], the U.S. Munitions List (USML) under the supervision of the Department of State's Directorate of Defense Trade Controls (DDTC).

This regulatory framework opened up an interpretative *vacuum (i*.e. a hole in legal regulation) that is difficult to manage. While everything that is not prohibited is permitted (and indeed the legislation in question does not prevent the production of 3D plastic weapons), it is also true that the post-9/11 legal framework takes the traceability of weapons through metal detectors as a significant issue. Instead, weapons produced with 3D printers escape these controls. This is/was the situation until the 24th of August 2022, when a new, and modernized, definition of "firearm" will come into force, after its publication in the Federal Register (supra 5).

So far the main point under discussion in front of the Federal Court was censorship issues regarding the dissemination of Mr. Wilson's instructions. In May 2015, he filed a petition against the US State Department in Federal Court in Austin, Texas, claiming that the censorship he suffered would be detrimental to several rights guaranteed to him by the Bill of Rights (Holden, 2016; Raven, 2021). In particular, this prohibition should involve:

- 1. the freedom to manifest thought, protected by the First Amendment of the US Constitution, on the basis that his pamphlet contained only software codes and therefore constituted neither an immediate danger nor a violation of international arms legislation;
- 2. the freedom to possess a weapon for self-defence, guaranteed by the Second Amendment;
- 3. the imposition of a sentence only after a fair trial, as established by the Fifth Amendment.

The issue is of great interest, not only because it concerns the regulation of the dissemination of products that can be manufactured with 3D printers, but above all, because it would appear to be the first time that the First Amendment of the US Constitution, a true cornerstone of US constitutional jurisprudence, has been used to uphold the ever more controversial Second Amendment on the right to possess weapons; however the Supreme Court of the United States denied the writ of certiorari[2].

However, the relevant question was: did freedom of expression or the need to protect national and international security prevail in this case? The court case concerned the possible necessity of the (temporary) blocking of the Internet dissemination of instructions for building a gun with a 3D printer between freedom of thought and the need to protect public safety. The issue at hand was based on the circumstance that with a 3D printer

[1] ITAR restricts the import or export of "defense articles" listed in the U.S. Munitions List (USML) including firearms and their components, as well as technical data required for the manufacture of such defense articles, under the supervision of the Department of State's Directorate of Defense Trade Controls (DDTC) (Huang, cit.).

[2] Defense Distributed v. U.S. Dep't of State, 838 F.3d 451 (5th Cir. 2016), cert. denied, 138 S. Ct. 638 (2018).

at hand and instructions readily available online, anyone can be enabled to self-build a firearm, at low cost and without the need for any licence or verification of possession of the firearm, which is not even traceable by current security systems, since it is made from plastic materials.

This was a factual situation at the centre of a heated debate: the US discipline presents a possible short-circuit among some of the absolute and founding values of American society and its legal system, in particular:

- 1. the absolute protection guaranteed to the freedom to express one's thoughts in any form and in any way (according to the 'free speech' doctrine guaranteed by the First Amendment of the United States Constitution.
- 2. the right of any person to possess a firearm at his or her disposal established by the Second Amendment of the same Constitution;
- 3. the stringent security and terrorism prevention regulations; and, finally,
- 4. the recurrence of mass murder by gun owners.

After that, and surprisingly, a 'settlement agreement' was reached between the Trump Administration and the Texan company 'Defense Distributed' regarding the authorisation of the internet dissemination of instructions for building firearms with a 3D printer, available for download as of Wednesday, 1st August 2018[3].

In order to prevent such publication from taking place, several district attorneys general have acted before federal courts, including those of California, Connecticut, Maryland, Massachusetts, New Jersey, New York, Oregon, Pennsylvania, and Washington. At the same time, other federal officials wrote to Attorney General Sessions and Secretary of State Pompeo urging them to block this initiative as it raises serious concerns for national as well as global security, since they are responsible for such blatantly harmful and unlawful information being made available to anyone via the Internet. According to the Attorney General of Pennsylvania, 'more than 1,000 people downloaded the instructions to make themselves a semi-automatic assault rifle'. On the contrary, the promoters of this initiative invoked the absolute necessity of the protection of freedom of expression. In a decision of 31 July 2018, Justice Robert S. Lasnik upheld the claims of the plaintiffs' prosecutors, based on both the likelihood of the realisation of irreparable danger and the likelihood of success on the merits, but also stated that this litigation poses serious problems with regard to the protection of free speech[4].

Finally, this controversy went in front of the United States Court of Appeals for the Ninth Circuit[5] established that the aforementioned International Security Assistance and Arms Export Control Act, and its subsequent amendments forbid judicial review on what is considered a "defense article" subject to such regulation.

So it seems to be back to the starting point, with the two fronts always open: on the one hand the contrast with the First Amendment, which seemed insurmountable. Indeed, First Amendment seemed to prevent any attempt to suppress the dissemination of the ghost guns (i.e. privately made firearms) instruction manual. On the other hand, the danger of the dissemination of ghost guns remained high. In any case, this (former) safety wall has been broken because the instructions are now available online through peer-to-peer sharing in the various (more or less) dark areas of the deep web.

The Biden administration, therefore, chose to take action on changing the definition of a weapon through a regulatory amendment published in the Federal Register[6]. This change introduced the definition of "privately made firearms", according to which "technological advances have also made it easier for companies to sell firearm parts kits, standalone frame or receiver parts, or partially complete frames or receivers to unlicensed persons, posing significant challenges to the regulation of frames and receivers and enabling prohibited indi-

---

[3] Settlement Agreement, Defense Distributed v. U.S. Dep't of State, 121 F. Supp. 3d 680 (W.D. Tex. 2015) (No. 15-CV-372-RP), 2015 WL 11022446. "(W)ith this settlement, DD's act of publishing the Liberator code online remains fully legal, although legislators have made several attempts to introduce bills that would criminalize such distribution.

[4] United States District Court, Western District of Washington at Seattle, 31.7.2018 State of Washington et al. v. United States Department of State http://www.wawd.uscourts.gov/news/temporary-restraining-order-state-washington-vs-united-states-department-state

[5] United States Court of Appeals for the Ninth Circuit, State of Washington v. U.S. Dep't of State, 27.4.2021 https://www.courthousenews.com/wp-content/uploads/2021/04/GhostGuns-9CA.pdf

[6] Definition of "Frame or Receiver" and Identification of Firearms, https://www.federalregister.gov/documents/2022/04/26/2022-08026/definition-of-frame-or-receiver-and-identification-of-firearms

viduals to easily make firearms at home, especially if aided by personally owned equipment or 3D printers. Ghost guns are not required by the Gun Control Act to have a serial number placed on the frame or receiver when made for personal use"[7]. (However, it does not change the main aspect, namely that plastic weapons remain untraceable and this is their main dangerous characteristic: being invisible, ghost guns, indeed.)

3. Intelligent weapons and humanitarian law

Before examining the regulatory framework of autonomous self-made weapons, we need to define the concept of autonomous weapons (AWS) and explore its international regulation.

Although there is no definition of AWS that is recognized internationally, it is generally agreed that, in order to be considered autonomous, a weapon must be able to act without meaningful human intervention (Verdiesen et al., 2021; Amoroso and Tamburrini, 2020). Taddeo and Blanchard offer the following definition: "*an artificial agent which, at the very minimum, is able to change its own internal states to achieve a given goal, or set of goals, within its dynamic operating environment and without the direct intervention of another agent and may also be endowed with some abilities for changing its own transition rules without the intervention of another agent, and which is deployed with the purpose of exerting kinetic force against a physical entity (whether an object or a human being) and to this end is able to identify, select and attack the target without the intervention of another agent is an AWS. Once deployed, AWS can be operated with or without some form of human control (in, on, or out of the loop). A lethal AWS is a specific subset of an AWS with the goal of exerting kinetic force against human beings*" (Taddeo and Blanchard, 2021).

International Humanitarian Law (IHL) does not discriminate between autonomous or non-autonomous weapons, therefore AWS is regulated by the law applicable to any other weapon. IHL limits the use of weapons in three ways: prohibiting or restricting specific weapons; prohibiting or restricting weapons in general; prohibiting or restricting the conduct of hostilities in general (Boulanin et al., 2021).

In addition to these three categories of law, the Additional Protocol I to the 1949 Geneva Convention, stipulates that "*In cases not covered by this Protocol or by other international agreements, civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and the dictates of public conscience*". There is therefore a general protection rule towards civilians and combatants, which is applicable to the use of AWS as well.

The general principles that must be followed according to IHL are the rules of distinction, proportionality, and precautions in attack (Davison, 2018). These rules might be difficult to abide by when AWS is involved, as there is no human intervention: for example, if a drone is sent to find the presence of humans in a certain area, and it is programmed to shoot when those humans are identified, it would be difficult to ensure that the attack is proportionate and that appropriate precautions have been taken.

In fact, some scholars have pointed out the limited capabilities of AWS to conform to IHL (Sharkey, 2012; Heyns, 2013; Suchman, 2016), and others have argued that, even assuming that they are capable of complying, they should not be employed (Asaro, 2012).

There is still no agreement on the definition of automatic or self-made weapon within comparative law scholarship, and the legal landscape presents some contradictions. For example, in France, human supervision is mandatory by law (Taddeo and Blanchard, 2021), whereas in German law AWSs completely exclude the human factor, apart from the human decisions about their employment (Geiss, 2017). The main debated issue is the definition of "human control" in using such weapons, and some efforts to reach an agreement on a common regulation are underway at the level of EU law (Barbé and Badeli, 2020). However, the lethal attack on former Japanese Prime Minister Shinzo Abe showed that the self-production of rudimentary homemade weapons will maintain a grey area, hidden behind a curtain of uncertainty. In our opinion, circumstances like these could be avoided only with effective social control.

Notwithstanding the many legal issues involved in the use of such technology, AWS is already employed in military conflicts. A recent report of the UN[8] disclosed that in Lybia "*Logistics convoys and retreating HAF were*

[7] Sect. B.

[8] Final report of the Panel of Experts on Libya established pursuant to Security Council resolution 1973 (2021).

subsequently hunted down and remotely engaged by the unmanned combat aerial vehicles or the lethal autonomous weapons systems such as the STM Kargu-2 (see annex 30) and other loitering munitions. The lethal autonomous weapons systems were programmed to attack targets without requiring data connectivity between the operator and the munition: in effect, a true 'fire, forget and find' capability. The unmanned combat aerial vehicles and the small drone intelligence, surveillance and reconnaissance capability of HAF were neutralized by electronic jamming from the Koral electronic warfare system".

4. AWS and biometric identification

A distinctive feature of AWS is the possibility to equip them with biometric identification technologies, such as facial recognition. AWS would then be able to recognize unique features of persons and uniquely identify them. This circumstance would allow AWS to hit a specific target without the help of a human.

The use of biometric recognition technology is regulated by international law, such as Convention 108+, GDPR, and *de iure condendo*, the EU AI Act. Because biometric data is considered personal data, it is, in fact, covered by privacy law.

The definition of biometric data is found in Article 29 Working Party (WP 29)'s Opinion no. 4/2007 (WP136): "*biological properties, behavioural aspects, physiological characteristics, living traits or repeatable actions where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability*"; the same document provides also a definition of biometric identification: "*The identification of an individual by a biometric system is typically the process of comparing biometric data of an individual (acquired at the time of the identification) to a number of biometric templates stored in a database (i.e. a one-to-many matching process)*", and points out that due to differences in the environment and in the equipment used, it is difficult to produce a biometric identification which is 100% accurate. The Working document on biometrics (WP80) of 2003 specifies that multiple biometric techniques exist: "*Firstly, there are physical and physiological-based techniques which measure the physiological characteristics of a person and include: fingerprint verification, finger image analysis, iris recognition, retina analysis, face recognition, outline of hand patterns, ear shape recognition, body odour detection, voice recognition, DNA pattern analysis and sweat pore analysis, etc. Secondly there are behavioural-based techniques, which measure the behaviour of a person and include hand-written signature verification, keystroke analysis, gait analysis, etc.".*

Like any other personal data in the EU, biometric data can only be processed if an appropriate legal basis exists and if the processing is adequate, relevant, and not excessive taking into consideration the purposes communicated to the data subject or the conditions of the re-use of data. In the case of AWS, the first legal issue is the legal basis for the collection and storing of the data used for the identification of the target, since it requires a match between the target's biometric data and a database of different biometric data used for the comparison. An additional legal issue resides in the way in which AWS models are trained: the training and testing datasets also require an appropriate legal basis for the processing.

However, the proposal published by the European Commission in 2021 for the regulation of AI provides for additional requirements related to biometric identification. In fact, it bans the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, and it strictly regulates the other uses of this technology, considering it as high-risk and arguing that "*technical inaccuracies of AI systems intended for the remote biometric identification of natural persons can lead to biased results and entail discriminatory effects. This is particularly relevant when it comes to age, ethnicity, sex or disabilities*" (Recital 33). Some examples of the new requirements are transparency obligations, quality management systems, data governance procedures, and human oversight measures.

5. A new threat to citizens: the ethical and legal debate surrounding DiDIY AWS

Self-produced AWS is only legal if employed according to the applicable laws and regulations, for example when employed for hunting by a licensed hunter, and the chance for this to happen depends on the differences in gun control legislation.

However, it is not the legal use of these devices that poses the major threats to citizens, but rather the circumstance that it would be very easy to employ them for illicit activities, since that they can be built in private fa-

cilities, and they are untraceable. Although the average citizen may not have the technological means and skills to build such devices, it is possible that in the future the number of people being able to self-produce them will increase: as noted by prof. Russell, "*building a lethal autonomous weapon is easier than building a self-driving car, since the latter is held to a far higher performance standard and must operate without error in a vast range of complex situations*"[9].

There is currently no prohibition on disclosing or publishing AWS 3D printing projects online in many countries, and it could even be a way for a legitimate company to prevent competitors from patenting their technology. The consequence of this freedom is that a high number of lethal AWS could be built by a small number of people, potentially becoming a weapon of mass destruction or genocide.

If equipped with biometric recognition, the dangerousness of AWS would constitute mostly in its capability of recognizing a specific target anywhere, making it impossible to hide, as the system would be able to find the subject even among a crowd of thousand people, or inside a building.

The ethical dilemma is not only related to the obvious danger of biometric identification, but also on the circumstance that specific targets would not be confirmed by a human being, but instead they would be selected by the AWS without human intervention or oversight, on the basis of the parameters set by the person who programmed it, which can be biased (Shoker, 2019). As we have seen, even biometric identification is not free from errors, and an accidental injury or death would occur without accountability, since no human being would be held responsible, at least *prima facie* (i.e. at first sight). Due to the untraceability of the weapon, many crimes could remain unpunished. Not to mention that letting an algorithm decide about human life is considered by many to be contrary to human dignity (Sharkey, 2019).

In addition, autonomous systems are not sensitive to deterrence strategies that humans enact in the attempt to stop unwanted escalation, potentially leading to inadvertent escalation and crisis instability (Wong et al., 2020).

Because of this, many open letters were signed from members of industry, NGOs, and academia, calling for a ban of these systems. Within the UN Convention on Certain Conventional Weapons (CCW), a Group of Governmental Experts on Lethal Autonomous Weapons to develop a new "normative and operational framework" was established in 2016, which laid down 11 principles on Lethal AWS (LAWS) in 2019. Among others, the principle of assessing the risk of cyber attacks, the risk of acquisition by terrorists, and the risk of proliferation were included.

However, despite a call for the ban of LAWS (Asaro, 2012), no international agreement has been reached so far, and the risk of self-production has not been addressed.

6. Possible solutions

The employment of AWS and the possibility of building it without the need of exceptional efforts poses great legal and ethical issues that cannot be solved just by delegating accountability to citizens. Without the intervention of States, self-made AWS will become more and more common.

Due to the inherent dangers of these systems, we believe that the most effective legal solution would be to ban them through a binding international instrument instead of attempting to regulate the matter at the national level. Even if all 11 principles drawn by the UN are respected and implemented, the risks for citizens would still remain significant.

In particular, we advocate for the prohibition of biometric recognition in LAWS, of disclosing projects online, and of building self-made AWS even for licensed individuals who intend to employ them for private use. If these situations are not criminalized, terrorist attacks may become more and more effective, as they will have "access to weapons of mass violence previously monopolized by the state" (Cronin, 2019).
Certainly, the choice of the legislator regarding how to address the threats posed by 3D-printed AWS must consider that terrorists might have access to the same type of technology by stealing it from the legitimate

[9] Article published by The Security Times and available at https://www.the-security-times.com/building-a-lethal-autonomous-weapon-is-easier-than-building-a-self-driving-car-a-new-treaty-is-necessary/ (last accessed 25/06/2022).

owners, by creating their own 3D projects, or by obtaining them on the black markets. A ban on the publishing of such projects might not be fully effective; on the other hand, it would not facilitate the spread of those weapons. However, if AWSes are banned *tout court*, it would be more and more difficult for terrorists to acquire them in alternative ways.

Regarding biometric identification technology, we believe that the risks would be mitigated if a stricter discipline regulates personal data. Recent cases regarding the legitimacy of online public content "scraping", used to train algorithms, highlight how the society is heading through the commodification of personal data, which could be acquired by terrorists in bulk to train their AWS. At least in Europe, administrative fines imposed to ClearviewAI, which collected pictures of unaware individuals, is a first sign of care towards the protection of citizens.

References

Amoroso, D., and Tamburrini, G. (2020). Autonomous weapons systems and meaningful human control: ethical and legal issues. Current Robotics Reports, 1(4), 187-194.

Asaro, P. (2012). On banning autonomous weapon systems: human rights, automation, and the dehumanization of lethal decision-making. International review of the Red Cross, 94(886), 687-709.

Asaro, P. (2019). Algorithms of violence: Critical social perspectives on autonomous weapons. Social Research: An International Quarterly, 86(2), 537-555.

Barbé E., Badeli D.(2020). The European Union and lethal autonomous weapons systems: united in diversity? In: Johansson-Nogués E, Vlaskamp M, Barbé E, editors. European Union contested: norm research in international relations. Cham: Springer; 133-52.

Boulanin, V., Bruun, L., and Goussac, N. (2021). Autonomous Weapon Systems and International Humanitarian Law: Identifying Limits and the Required Type and Degree of Human–Machine Interaction.

Cronin, A. K. (2019). Power to the People: How Open Technological Innovation is Arming Tomorrow's Terrorists. Oxford University Press.

Davison, N. (2018). A legal perspective: Autonomous weapon systems under international humanitarian law. UNODA Occasional Papers, 30, 5-18.

de Ágreda, Á. G. (2020). Ethics of autonomous weapons systems and its applicability to any AI systems. Telecommunications Policy, 44(6), 101953.

Geiss, R. (2017). Lethal Autonomous Weapons Systems: Technology, Definition, Ethics, Law & Security. Federal Foreign Office.

Haner, J., and Garcia, D. (2019). The artificial intelligence arms race: Trends and world leaders in autonomous weapons development. Global Policy, 10(3), 331-337.

Heyns, C. (2013). Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, A/HRC/23/47. New York: United Nations.

Holden, G. E. (2016). How Far Should the Rights to Post 3D-Printed Handguns Extend: Does the Government Infringe upon Constitutional Rights by Requiring The Removal Of 3d-Printable Handgun Blueprints, 18 Fla. Coastal L. Rev. 279.

Huang, A. (2022) 3D Printed Speech: 3D-Printer Code Under Constitutional Scrutiny, HARV. NAT'L SEC. J. ONLINE, https://harvardnsj.org/wp-content/uploads/sites/13/2022/02/3D-Printed-Speech-Constitutional-Scrutiny.pdf

Pasquale, F. (2020). New Law or Robotics: Defending Human Expertise in the Age of AI, The Belknap Press, Cambridge Massachusetts, London UK, Chap. VI.

Raven, W. A. (2021). Packing Plastic: How A Federal Ban On 3d Printed Firearms May Protect The Public While Retaining Constitutionality, The Journal of High Technology Law.

Sharkey, A. (2019). Autonomous weapons systems, killer robots and human dignity. Ethics and Information Technology, 21(2), 75-87.

Sharkey, N. (2012). Automating warfare: Lessons learned from the drones. Journal of Law, Information and Science, 21(2), 140.

Shoker, S. (2019). Algorithmic Bias and the Principle of Distinction: Towards an Audit of Lethal Autonomous Weapons Systems. Digitization and Challenges to Democracy, 41.

Suchman, L. (2016). Situational awareness and adherence to the principle of distinction as a necessary condition for lawful autonomy. In Panel presentation at CCW Informal meeting of experts on lethal autonomous weapons, Geneva, April 12, 2016.

Taddeo, M., and Blanchard, A. (2021). A comparative analysis of the definitions of autonomous weapons.

Verdiesen, I., Santoni de Sio, F., and Dignum, V. (2021). Accountability and control over autonomous weapon systems: A framework for comprehensive human oversight. Minds and Machines, 31(1), 137-163;

Wong, Y. H., Yurchak, J. M., Button, R. W., Frank, A., Laird, B., Osoba, O. A., and Bae, S. J. (2020). Deterrence in the age of thinking machines. RAND Corporation Santa Monica.