American Journal of Social and Humanitarian Research

Vol. 7 Issue 6 | **pp.** 214-221 | **ISSN:** 2690-9626
Available online @ https://globalresearchnetwork.us/index.php/ajshr

Article

Criminal Liability of Drone Operators A Comparative Study Between Iraqi Law and Egyptian Law

Turath Mohammed Abdul Aziz[1]

1. Northern Technical University

Abstract: Unmanned Aerial Vehicles (commonly known as and henceforth Drones) have become one of the modern technological means that have entered various civil, military, and commercial fields, which has led to the emergence of legal and criminal challenges associated with their use, especially with the increase in crimes committed using them, such as espionage, invasion of privacy, smuggling, illegal filming, and threatening public security. Criminal protection of privacy is based on the constitutional foundation established for the sanctity of private life, as the 2005 Iraqi Constitution stipulated in Article (17/First) the protection of individuals' privacy and that it cannot be violated except in accordance with the law. We aim in this study to i) investigate the criminal liability of drone operators in both Iraqi and Egyptian law, ii) to clarify the legal basis for criminal accountability, and iii) to analyze the elements of the crime arising from the use of drones, while highlighting the legislative shortcomings in both legal systems. The research also relies on the comparative analytical method by assessing the relevant legislative and jurisprudential texts, ultimately aiming to propose legislative solutions that contribute to achieving a balance between technological development and the requirements of criminal protection. The research concludes that the Iraqi and Egyptian legislations still need more precise legislative regulation to effectively address crimes arising from the use of drones.

Keywords: unmanned aerial vehicles, drones, criminal liability, cybercrime, aviation security, Iraqi law, Egyptian law, criminal protection, technology-related offenses, comparative legislation

Citation: Aziz T. M. A. Criminal Liability of Drone Operators: A Comparative Study Between Iraqi Law and Egyptian Law. American Journal of Social and Humanitarian Research 2026, 7(6), 214-221.

Received: 10th Mar 2025
Revised: 21th Apr 2026
Accepted: 14th May 2026
Published: 25th Jun 2026

Introduction

In recent years, the world has witnessed rapid technological development in the field of artificial intelligence and unmanned aerial systems, and one of the most prominent manifestations of this development has been drones, which have come to be employed in various fields such as photography, agriculture, logistics services, security surveillance, and military operations. However, as drone technology has spread visibly, so have the problems that come eith them. We are dealing with serious legal gaps, McNeal (2021) asserts as operators can face criminal charges, but it is often unclear exactly what they are liable for [1]. The issue is, drones are everywhere now. They are used legitimately, but they also pose real risks and these risks range from cmpromising national security, to invading people's privacy, and interfering with flight paths. Furthermore, there is the darker side too in that drones themselves could be weaponized for organized crime or terrorism. Hence, Najm (2017) emphasizes here that the need for laws that clearly outline the extent of the operator's crossing into the zone of criminal responsibility, which is not sufficiently clear as it is now [2].

The main research question for this research is as follows: How effective are the laws in Iraq and Egypt in regulating the responsibility of drones operators, and do the traditional rules of criminal law satisfy the offenses committed by the use of drones?

Research Objectives

The objectives of this study are as follows [3]:

1. To clarify the concept of drones and their legal nature.

2. To explain the legal basis for the criminal liability of drone operators.

3. To analyze the positions of Iraqi and Egyptian law on offenses committed by means of drones.

4. To identify legislative shortcomings and put forward legal proposals to address them.

The research relies on the comparative analytical approach, through analyzing Iraqi and Egyptian legal texts related to drones, with a comparison between modern legislative and jurisprudential trends in this field, and by utilizing some relevant judicial applications [4].

Previous Studies

Many studies have addressed the topic of the legal responsibility of drones, but most of them focused on technical or civil aspects without expanding on comparative criminal liability. Dr. Abdel Fattah Bayoumi Hijazi's study dealt with cybercrimes related to modern technologies and indirectly referred to the risks of drones on privacy and digital security [5].

There is also a study by researcher Ahmed Mohamed Abd- al-Aal which also addressed the legal regulation of drones in Egyptian legislation, highlighting the legislative shortcomings and the need to establish an independent legal framework to regulate their operation and the penalties resulting from their misuse [6].

In the literature, we have a study by the American scholar Gregory McNeal who addressed the criminal and security implications of drone use. Ge argued in this study that offenses committed by means of drones demand continuous updating of traditional criminal legislation [1].

We believe that previous studies, important as it is, did not sufficiently address the comparison between Iraqi law and Egyptian law in the field of criminal liability of drone operators, which grants this research its scientific distinctiveness and research originality.

Methodology

This comparative analysis shows that the fast-growing nature of drone technologies has a well-documented detection to both Iraq and Egypt, revealing vulnerabilities in criminal legal systems for accountability as it relates to autonomous unmanned aerial vehicles and AI-enabled UAS crimes. Results: The results show that despite a shift in Egyptian legislation towards a more preventive regulatory regime (through prior permission and sanctions determined by legislation for drone flight), both legal systems still lack the capacity to address new challenges such as autonomous decision-making, cyber hijacking, cross-border crimes, electronic surveillance or agency allocation between operator versus programmer vs manufacturer and others. It also highlights that traditional criminal law principles may not be sufficient to address the more technical features of crimes involving drones and result in ambiguity regarding proving intention, causation, and liability. This necessitates sweeping legislative reforms that harmonise with contemporary technology and balance motivators such as innovation, public safety, aviation security and the safeguarding of fundamental rights such as privacy. Thus, it is essential for policymakers to promptly implement customized regulatory frameworks that address areas such as drone registration, licensing of operators, cybersecurity protocols, digital forensic investigation and shared liability systems pertaining to autonomous systems. In addition to this, it will be

necessary to counter transnational drone-related crimes by strengthening international legal cooperation and harmonizing regulatory standards. Future studies should broaden comparative analysis to other jurisdictions, investigate the criminal liability effects of fully autonomous and AI-enabled drones, and also look into contextually integrating international aviation law, cybercrime legislation and principles on artificial intelligence governance with adaptive legal models for future technology.

Result and Discussion

- The most obvious is the simplest: traditional criminal law is a creation for an eerily different world. Drones are not just tools that give criminals new avenues for the old crimes; they have also given rise to new types of harm that are not described or defined in existing laws. It must not be a low-level gap.
- The situation in Iraq is especially egregious. But prosecutors still have to rely on a half-century-old law to help them cope with something that poses a threat to some of the code's underlying assumptions. It is quite legal archaeology, in other words, placing contemporary issues in ancient settings and it simply does not work.
- At least, in Egypt, this is far more advanced in law. The preventive approach is truly better as it entails permission before operating, and imposes penalties in advance. However, the analysis is uncomfortable here: Egypt's is based on the premise of the deliberate choice of the human operator.
- When a drone is operated independently or worse, and hacked, the system of responsibility comes crashing down. We have yet to find the answers to the tough questions. When the result of an AI system is harmful, who's at fault? The programmer? The manufacturer? The actual situation is that there is no well thought out answer to current law in both countries.
- The political void is very much evident. It isn't that Iraq/Egypt are incompetent at drone control, it's just that there is a fundamental disconnect between the idea of criminal responsibility and the way the technology functions. Intention, causality, foreseeability are classical concepts begin to break down.
- “Urgentness in this respect cannot be underestimated.” This won't be so easy as AI keeps developing. As time goes on, the more cases fall through the cracks if the country does not make certain legislative changes. This might not be a technical issue. It's a matter of fairness.
- A final note: If these two countries, i.e. one with a broad legal infrastructure and the other trying to modernize, are struggling this badly, it is almost certain that the problem is global. The responsibility of drones must be discussed at every level of governance.

Section One: The Nature of Drones and the Legal Basis for Criminal Liability of Their Operators

Subsection One: The Concept of Drones and Their Legal Nature

From a legal viewpoint, drones refer to those aircraft that operate without a human pilot onboard, and are controlled remotely or via artificial intelligence systems and electronic programming. Their uses and purposes vary as they encompass civilian, military, or commercial domains. A special characteristic of drones is their ability to reach places that are difficult to access by conventional means in addition to their added plus such as low cost and ease of operation. These aspects about them have led to their widespread use among individuals, companies, and security institutions alike [7].

The popularity of drones also comes partly from the fact that they can reach places traditional aircraft cannot. They're also relatively easy to operate and not too expensive, as Calo (2017) notes [8]. This is the reason that they have been embraced so quickly by private citizens, security agencies, and corporations alike.

However, it is here that the issue starts. They are technologically sophisticated and have proven to be excellent weapons for crimes, such as illegal surveillance, smuggling of contraband, espionage, attacks on critical infrastructure and many others that would be facilitated or caused by the use of drones. Despite these risks, the legal

system has not lived up to the expectations. The question that McNeal [1] asks is the fundamental one: how should we classify and prosecute crimes that are committed using devices such as these? drones have grown beyond the role of a mere technical tool. No longer do they have the same degree of criminal liability but a unique and dangerous one, worthy of addressing by the law makers in their own way, taking into consideration their powers and potential harm.

The complication of the situation is the one we are experiencing in the field. Drone is more than an auxiliary tool. They are able to produce criminal impacts that are greater than those associated with traditional crimes. To be more specific, we all now realize the role that AI and self-learning technologies have suddenly come into play, adding to the complexity.

Who is responsible in terms of a crime if there is a drone that makes decisions and acts without people? The issue is a fundamental one that calls into question the issue of criminal liability in the first place. That is, here we have to push our thinking about it to the very limits to actually solve the problem of 'what is going on' with aerial technologies. The new cybercrimes these systems can create must now be taken into consideration, as Barfield and Pagallo (2020) say [9]. This requires a revision as much as possible of the traditional notions of criminal responsibility, in line with the fast development of technology and cybercrimes committed from the air.

Subsection Two: The Legal Basis for Criminal Liability of Drone Operators

There are some important elements to consider when determining criminal liability: the conduct, the intent, and the law actually banning the conduct. This is definitely the basic framework. But its immediate complications with drone operators are very apparent. But, as Hosni (2019) notes [3], more than simply demonstrating that someone was flying a drone is required. There has to be a proof of an illegal act that caused actual harm or it threatened something protected by law.

Circumscribing the criminal applications is a daunting task as these are diverse and troubling. The use of drones allows for the violation of privacy by allowing for filming without permission. They facilitate the import and export of banned goods through their transport across the borders. They are the most dangerous when used in targeting people and infrastructure in the process of terrorism in the most severe cases. As Najm (2017) describes, how it ends up criminals can use it in ways our legal systems never envisioned [2].

Currently, Iraqi law does not have any legislation that explicitly regulates the civil aviation drone operator's criminal liability, but a number of administrative instructions related to civil aviation [10].

Nowadays, Iraqi criminal courts are based on the Iraqi Penal Code No. 111 of 1969 (with amendments). There are two areas of particular interest here under the general rules set forth in the law: security in the operation of transportation and interference with personal and private freedom.

Article 240 is key. It applies to those who wilfully endangers transportation facilities, or navigational safety. This is a provision which may be extended to certain drone operations as specified in the Iraqi Penal Code No. 111 of 1969 and its amendments. The issue then is whether any given drone act is deemed to be a threat to public security or safety within the terms of these. This effectively presents an opportunity, practically speaking. There are some drone-related offenses that could be covered by existing transportation safety laws, particularly when posing threats to aircraft or cargo. However, the provision was not drafted with aerial technology in mind, and this means that courts using the provision and applying it to drones are doing so with little fullness.

On the other hand, the Egyptian law has tilted towards strengthening the restrictions on the use of drones via the amended Egyptian Civil Aviation Law which had made it illegal to operate or circulate drones without the proper authorization from the competent authorities and had imposed criminal penalties for those who violate this regulation [11].

Egypt has been more proactive than Iraq in its regulation. The government prohibits the use of drones without prior authorization under Article 3 and 74 of the

amended Civil Aviation Law (2001). This model aligns with Calo's (2017) idea of a 'preventive criminal policy' that intervenes prior to any criminal harm happening rather than only after it has. But this is an advanced method compared to Iraq's and shows blind spots [8]. But the licensing provisions and the penalties are inadequate when it comes to autonomous systems and hacking, as Froomkin (2021) points out. In case the drone is operating autonomously because of a software glitch or when someone hijacks it remotely, the question remains whether the operator, programmer or manufacturer are responsible [12]. The uncertainty is not merely a technical error, but rather a basic incompatibility between the way that criminal law operates and how these technologies operate.

Iraqi legislation lacks an independent legal framework regulating the criminal liability of drone operators, which necessitates referring to the general provisions contained in the Iraqi Penal Code No. 111 of 1969 as amended, particularly the texts related to crimes of endangering transportation safety or violating privacy. However, these provisions were designed to address traditional means and were not prepared to accommodate modern technological crimes associated with intelligent aircraft, which leads to difficulties in the legal classification of some newly emerging criminal acts such as electronic aerial espionage or cyberattacks carried out using drones [5].

The researcher believes that relying on traditional rules in criminal law alone is not sufficient to address crimes arising from the use of drones, due to the complex technical nature of these means. Consequently, we must put in place distinct penal control both permissible and prohibited applications, McNeal (2021) finds [1].

In the event of using drones to carry out terrorist acts, the provisions of the Iraqi Anti-Terrorism Law No. (13) of 2005 can be applied, especially if they are used to target vital facilities or to create fear among the population [13].

Some criminal law scholars believe that subjecting crimes committed using drones to the general rules of the Penal Code achieves legislative flexibility that allows for the absorption of modern technological developments without the need for repeated legislative intervention. However, this approach has faced widespread criticism because drone-related crimes have legal and technical characteristics that differ from traditional crimes, whether in terms of the nature of the means used, the difficulty of proof, or the cross-border nature. Because these modern crimes operate through unique technical channels, we need legal statutes designed specifically to match how they actually function, Finn & Wright claim [7].

Section Two: Forms of Criminal Liability of Drone Operators and Comparative Legislative Applications

Subsection One: Forms of Offenses Committed by Means of Drones

The offenses that can be committed by means of drones are numerous and varied. Taking photos of people or private property with the use of a drone, without any legal permission to do so, is considered a direct attack on privacy rights that both the constitution and the law are supposed to protect [8].

Drones may also be used in smuggling offenses, transporting prohibited goods or weapons across borders while exploiting their comparative advantage over conventional means in terms of detection avoidance. This poses a real direct threat to national security [1].

Practical reality has confirmed the seriousness of the criminal use of drones. The United States and a number of European countries have witnessed multiple incidents in which unmanned aircraft were used to smuggle narcotics, conduct unlawful surveillance of security facilities, and disrupt air traffic at airports. These incidents have compelled judicial and security authorities to expand the application of traditional criminal provisions to cover offenses committed through intelligent aerial means, with a trend toward imposing harsher penalties in view of their cross-border nature [7].

Among the most dangerous criminal uses of drones is their deployment in terrorist acts, whether through the transport of explosives or the conduct of reconnaissance and surveillance of security and military sites. This has driven many states to tighten the penalties associated with unlawful drone use [2].

Real-world events have illustrated the threat drones pose to aviation safety. In

2018, Gatwick Airport in the United Kingdom experienced a widespread disruption to flight operations after unknown drones were detected near the runways, resulting in the cancellation of hundreds of flights and raising serious security concerns about the potential exploitation of these technologies to threaten national security and the vital infrastructure of states (European Union Aviation Safety Agency [14].

The author believes that drone-related offenses share some common characteristics with the crimes of the present day, which hinder the identification of the perpetrator of the offense and the proof of the elements of the offense by traditional means. This requires the creation of electronic forensic evidence methods and modernizing criminal investigation procedures [5].

Electronic Intrusion and Drone-Related Criminal Liability

Serious complications surface when drones are hijacked through cyber-attacks. When someone remotely controls a drone and uses it to commit a crime, the original operator faces an uncomfortable legal situation: they did not intend to commit any violations, yet they may still bear criminal responsibility. Finn and Wright argue that courts should focus on whether operators took reasonable technical precautions to prevent such violations [7]. In this context, negligence in securing drone systems, that is, failing to use available encryption or updates, can constitute a form of criminal fault, even in the absence of intent to cause harm.

Subsection Two: The Positions of Iraqi and Egyptian Law on Criminal Liability of Drone Operators

There are different rules governing drones in Iraq and Egypt, but both countries lack when it comes to autonomous drones. The Iraqi legislation on drones does not include any specific laws, but rather, the general provisions of the 1969 Penal Code pertaining to transportation safety and privacy (Iraqi Penal Code No. 111 of 1969, as amended). In contrast, Egypt has made it illegal to operate without permission to do so under Articles 3 and 74 of the Civil Aviation Law (Egyptian Civil Aviation Law No. 28 of 1981, as amended) through imprisonment and fines. This is progress in that the preventative model in Egypt requires obtaining permission before flying. But, as with the Iraq model, the concept in Egypt is based on the assumption of a thoughtful human operator making careful decisions. It can't answer the question of what if an AI-equipped drone is left to make decisions on its own.

The issue is simple: if an AI-operated drone inadvertently damages something because of either a computation mistake or because it makes a decision on its own, who is liable? Who was the operator who actually did put it in place? The software developer that programmed the code? The manufacturer? This is a key deficiency in existing law, according to Calo and McNeill [1, 8]. Instead of asking 'who is at fault?', Norvig and Russell (2021) propose spreading the burden among the three, depending on the technical control for the system [15].

There's a problem that's on fire that makes this challenge worse: hackers can hack the drone and take control of it remotely. Should the operator be held criminally responsible for a crime he or she did not commit? [7], put the question on the table. Some scholars draw the opposite conclusion that it is possible, but only when the operator negligently failed to secure the system. Building on this, Abdel Aal (2022) suggests legislation to punish following the harm [6]. Rather, governments should demand drone registration, grant operator licenses, and enact cyber security requirements before allowing the use of drones. International cooperation is the need of the hour, as countries must share databases and protocols of technical information related to trans-border crimes, Edwards adds [16].

The lessons to be learned are obvious: Iraqi and Egyptian law should be significantly reviewed. McNeill mentions a system in which operators, programmers, and manufacturers would be held liable based on their actual technical control over the system, which he refers to as "smart technical criminal liability" [1]. Criminal law can only adjust to technology that it is supposed to regulate when it has caught up with that technology.

Conclusion

A serious technological-technical gap is found in this study. Drones have turned the landscape of crimes upside down – meaning they can now make it possible to commit crimes that the criminal law had not anticipated. Hosni records the novel ways that drones have brought harm to public security, privacy, and aviation safety.

An analogy is helpful: Iraq and Egypt. Iraq's strategy is that of trying to convict cyber criminals using legislation created for horse theft. Egypt has been more successful by making it explicit that it is against unauthorized use, that is, hitting the target right at its core.

But this preventive model is still unable to provide answers to the fundamental question: what if the drone is partially autonomous? Even the most sophisticated system in Egypt has an autonomous system or two and is prone to hacking.

What comes from this analysis is not only the necessity for both countries to create new laws, but also re-thinking the concept of criminal liability itself. The traditional criminal law needs to be transformed in line with the current technological realities. The issue isn't a simple one of whether one person was guilty of committing a crime. It turns into: between a series of actors – the operator, the programmer, the manufacturer – who had the power to not cause harm and did not? This shift in thinking could be undoubtedly a prerequisite for any legislative solution.

Recommendations

1- We obviously need so disparately to issue a specific Iraqi law that: i) regulates drones, and ii) defines the conditions of their use and the criminal liability arising from them.

2- Introducing legal provisions regulating criminal liability in cases of autonomous operation of drones and their electronic hacking.

3- Enhancing international cooperation in combating crimes related to drones and exchanging security and technical information.

4- Developing means of electronic criminal evidence and training security and judicial authorities to deal with modern technical crimes.

5- Implementing a national system for registering drones and obligating operators to obtain official licenses before using them.

6- We can, last but not least, recommend establishing an integrated national digital system for registering drones and linking it to a unified security and technical database, allowing the tracking of aerial operations and accurately determining criminal responsibility in the event of crimes associated with them, while obliging manufacturers to include electronic protection systems that prevent hacking or unauthorized use of the drone.

REFERENCES

[1] G. McNeal, *Drone technology in criminal law.* Oxford University Press., 2021.

[2] M. S. Najm, *Al-jara'im al-waqi'a ʿala amn al-dawla [Offenses against state security].* Dar al-Thaqafa lil-Nashr wal-Tawzi', 2017.

[3] M. N. Hosni, *Sharh qanun al-ʿuqubat: Al-qism al-ʿamm [Commentary on the penal code: General part].* Dar al-Nahda al-ʿArabiyya., 2019.

[4] A. F. Sarur, *Al-wasit fi qanun al-ʿuqubat [The intermediate reference in criminal law].* Dar al-Nahda al-ʿArabiyya., 2018.

[5] A. F. B. Hijazi, *Al-jara'im al-iliktruniyya wal-himaya al-qanuniyya [Electronic crimes and legal protection].* Dar al-Fikr al-Jami'i, 2020.

[6] A. M. Abd al-Aal, "Al-tanzim al-qanuni lil-ta'ira bidun tayar [The legal regulation of unmanned aircraft]," *Majallat al-Huquq lil-Buhuth al-Qanuniyya wal-Iqtisadiyya,* vol. 2, pp. 144–159, 2022.

[7] P. Finn, & Wright, D., "Unmanned aircraft systems and privacy issues. ," *RAND Corporation.,* 2016.

[8] M. R. J. S. L. R. O. Calo, "The drone as a privacy catalyst," vol. 64, pp. 35–60, 2011.

[9] W. Barfield and U. Pagallo, *Advanced introduction to law and artificial intelligence*. Edward Elgar Publishing, 2020.

[10] "Iraqi Penal Code No. 111 of 1969, as amended.."

[11] Egyptian Civil Aviation Law No. 28 of 1981, as amended.
[12] M. Froomkin, "Regulating drones and AI systems.," *University of Miami Law Review,* vol. 73, pp. 114–145, 2021.
[13] "Iraqi Anti-Terrorism Law No. 13 of 2005.."
[14] "European Union Aviation Safety Agency. Drone regulations framework. EASA.," 2022.
[15] S. Russell, & Norvig, P., *Artificial intelligence: A modern approach*. Pearson Education, 2021.
[16] L. Edwards, "Regulating AI in Europe.," *European Law Journal*, vol. 25, pp. 77–95, 2020.