民用无人机领域数据与飞行安全法律规制研究*

黄煦淇, 洪 晟

(北京航空航天大学 网络空间安全学院, 北京 100191)

摘要: 无人机技术是当今工业互联网发展的助力之一, 尤其是 5G 技术与无人机技术的结合成为推动工业向数字化转型升级的重要力量。但是, 在无人机大规模应用的同时, 也不能忽视其给行业带来的风险与挑战。主要讨论民用无人机存在的隐私侵权问题及其造成的数据安全隐患和“黑飞”问题, 并对比中外法律法规提出有关法律体系建设的建议。

关键词: 民用无人机; 数据安全; 公民隐私; 黑飞

中图分类号: F49

文献标识码: A

DOI: 10.19358/j.issn.2096-5133.2022.06.006

引用格式: 黄煦淇, 洪晟. 民用无人机领域数据与飞行安全法律规制研究[J]. 信息技术与网络安全, 2022, 41(6): 31-35.

Research on legal regulation of data and flight safety in civil UAV field

Huang Xuqi, Hong Sheng

(School of Cyber Science and Technology, Beihang University, Beijing 100191, China)

Abstract: UAV technology is one of the driving forces for the development of industrial Internet. In particular, the combination of 5G technology and UAV technology has become an important force to promote the transformation and upgrading of industry to digital. However, in the large-scale application of UAV, the risks and challenges brought to the industry can not be ignored. This paper mainly discusses the data security and data governance caused by the privacy infringement and illegal flight of civil UAV, and puts forward suggestions on the construction of legal system under the comparison of relevant laws and regulations in China and foreign countries.

Key words: civil UAV; data security; privacy infringement; illegal flight

0 引言

工业互联网作为信息化与工业化深度融合发展的产物, 是工业与制造业数字化、智能化发展的基础。无人机凭借其灵活性强、便捷性等优势, 为工业互联网发展提供重要助力^[1]。5G 工业无人机的出现, 其作为 5G+互联网的产物, 代表了产业数字化转型升级的方向。民用无人机市场逐渐扩大, 在航拍、植保、物流、巡检、救援等领域发展迅速^[2]。然而, 在无人机大规模应用的同时, 无人机飞行安全问题为行业发展带来了困扰。消费级无人机的使用对象以人为主, 经常需要对人进行拍摄跟踪, 使得公共空间与个人隐私空间的界限变得模糊, 威胁公

民的隐私安全。工业级无人机方面, 常有违法违规的“黑飞”行为, 扰乱航空行程, 极大地破坏公共安全和公共秩序。

本文主要研究针对民用无人机隐私侵权和“黑飞”等问题, 结合国内外相关领域治理经验, 对目前国内法律法规尚不完善的地方给出意见和建议, 从法律层面为无人机产业发展提供长远保障。

1 民用无人机领域现存风险

1.1 隐私侵权

近年来, 民用无人机侵犯公民隐私事件频发, 公民个人隐私安全受到重大挑战。

1.1.1 民用无人机隐私侵权风险

民用无人机目前在农作物检测、航拍摄影、图

* 基金项目: 北京航空航天大学研究生精品课程建设项目(403918)

形测绘、快递运输等领域有较高的使用率。常用的无人机为消费级无人机,主要在个人隐私保护性需求较高的居民住宅区或人口流量大、人员密集的商业区保有并使用。高使用率与易探查的特点,为利用无人机获取他人隐私信息提供了条件。由于民用无人机大多是微型、轻型无人机,体积小,隐蔽性强,因此很难被发现;同时,无人机的空中悬停技术结合装载的高清相机,能拍摄到距离较远的微小事物^[3],这些优势使得其对隐私的获取能力显著增强。

无人机对公民隐私的侵害和监控,一方面会对公民的日常生活造成影响,比如对公民隐私的记录和泄露会给其生活造成麻烦和骚扰;无处不在的监视感会给公民带来不适和不安全感,造成不必要的心理压力,甚至可能造成社会信任恐慌。另一方面,存在隐私数据被泄露或非法利用的风险。根据《中华人民共和国数据安全法》,数据被非法利用破坏了数据的机密性,隐私数据被泄露对数据安全造成了极大威胁。

1.1.2 民用无人机隐私侵权特殊性

无人机对他人的隐私侵权有其特殊性。首先,对侵权者来说,对他人的隐私侵权具有轻易性、全方位的特点^[4]。相较于传统摄像机拍摄的诸多条件限制,民用无人机能相对轻易地入侵他人的私人领域,而不需要侵权者本人进入。而随着5G与无人机的结合,高速率、低功耗的5G网络使得无人机的远距离控制优势增强^[5],一旦侵权者锁定了其侵权对象,便可以利用无人机进入其不被允许的领域来获取其想获得的隐私信息,甚至实施长期监视。其次,民用无人机的隐私侵权一般都是在被侵权者无意识的情况下进行的,即“无感侵害”,具有隐蔽性和滞后性,即使被侵权者发现了自己的隐私正在被侵犯,由于无人机侵权“人机分离”的特性^[6-7],很难通过无人机确定侵权者,使得用法律武器保护自己的隐私权变得困难。

1.2 无人机“黑飞”

无人机“黑飞”指的是违反现有法律法规进行无人机飞行活动的行为^[8]。根据相关法律规定,除微型、轻型无人机外其他民用无人机的飞行活动需要驾驶员取得安全操作执照,同时其无人机的飞行活动需要登记备案。未经备案的民用无人机飞行以及未取得操作资质的驾驶员对公共安全与社会秩

序有较大风险。2017年4月,成都双流机场在17天内多次有无人机在空中接近正常飞行的民航客机,威胁航班的飞行安全,造成大量航班备降^[9]。由此可见,民用无人机“黑飞”带来的危险不容忽视,应该被严令禁止。

2 国内相关法律法规

2.1 我国民用无人机隐私侵权法律

目前民用无人机领域的法律主要集中在无人机飞行方面^[10],基本没有涉及民用无人机的隐私侵权问题。《低空空域使用管理规定(试行)》《轻小型民用无人机飞行动态数据管理规定》等条例涉及了民用无人机侵犯公民隐私权的问题,但是没有明确的隐私侵权定义和侵权后相关处罚规定等,只有“承担相应的民事赔偿责任”^[11]这样笼统模糊的规定。之所以会出现这样的局面,主要有以下两个原因:

(1) 法律位阶较低

目前针对民用航空领域的上位法只有《中华人民共和国民用航空法》(简称《民用航空法》),虽然经过了多次修订,但其中并没有包括针对无人机隐私侵权的相关条款,使得无人机侵权事件只能比照民用航空器的规定进行处理。但由于民用无人机隐私侵权的特殊性,使得实际处理变得困难。

(2) 监管部门不清

虽然有法律法规对我国民用无人机管理的领导机构、工作机制,以及不同机关、部门间的管理职责进行了规制^[12],但对于部门职能界定与权责划分依旧模糊,且该条例没有针对民用无人机侵犯隐私权相关问题的规制,使得监管变得更加复杂难以处理^[7]。

2.2 我国无人机飞行管控法律

《无人驾驶航空器飞行管理暂行条例(征求意见稿)》对无人机未来发展及管理做出规定,同时首次对违规飞行采取具体惩处措施,体现出国家对无人机问题高度重视。该条例对民用无人机的飞行进行了全面规定,专门点出了“对在民用航空使用空域范围内或对以上空域内运行存在影响的民用无人驾驶航空器进行空中交通管理”,对无人机“黑飞”进行法律约束。《民用无人驾驶航空器系统驾驶员管理暂行规定》则主要对民用无人机驾驶人员进行规范管理,从行业协会、局方对驾驶人员进行监督

管理和资质认定^[11]。即便如此,对无人机的追踪及侦查尚且处于有心无力的局面。

3 国外相关法律法规

3.1 美国民用无人机隐私侵权法律

美国针对民用无人机侵权方面的法律较为完善,有相关立法并进行监督管理。2015年,美国电信和信息管理局建立了《民用无人机隐私安全指南》,它是专门针对民用无人机隐私侵权的文件^[13],其对民用无人机侵犯公民隐私进行了清晰的界定,并规定了明确的处罚标准,建立了民用无人机下的隐私保护体系。除了国家层面对民用无人机隐私侵权进行法律文件约束之外,美国地方各州也出台了一系列民用无人机隐私侵权的相关法律法规。比如佛罗里达州颁布的《免受监视自由法案》明确规定,个人禁止未经授权对他人及其财产进行录像^[14];得克萨斯州出台法律规定,禁止任何人使用无人机在未经允许的情况下对他人及其财产进行图像记录,并对违反规定的行为制定了明确的处罚规定^[15]。国家和各州都针对民用无人机隐私侵权进行法律条例制定,避免出现“无法可依”的局面。

3.2 美国民用无人机飞行管控法律

2015年,美国联邦航空局要求所有小型无人机购买者都要进行实名注册^[8],使得无人机追踪更加方便。2016年,为了管制广泛使用的消费级无人机,美国联邦航空管理局又颁布了关于小型无人机的监督条例。该项规定的重要之处在于对无人机操作资格进行放宽处理,驾驶此类无人机不再需要经过严格测试的飞行执照,只需要通过有关部门的审查就能获得非永久性的使用证书^[16]。这一举措使得无人机操作者能更方便地进行合法操作飞行,一定程度上缓解了“黑飞”的现象。除此之外,还出台了用户无人机规范使用APP,使无人机操作者能方便快捷地确认无人机飞行的合法区域和高度^[16]。

4 完善现行法律法规建议

针对上述民用无人机领域存在的安全风险需要加强相关法律、制度和规范方面的建设。

4.1 隐私侵权

4.1.1 建立隐私权合理期待原则

民用无人机隐私侵权除了容易入侵公民私人领域外,在公共场所也很容易造成他人隐私侵犯。目前,我国尚未明确规定公共场所具有隐私权,还

没有对公共场所隐私权的判定标准问题作出任何规定^[17]。借鉴国外较为完善的民用无人机隐私保护经验,建议明确公民在公共场所具有隐私权,并引入合理期待原则作为判定隐私权被侵害的标准,为判定民用无人机在公共场所侵害公民隐私提供较为明确的法律制度保障。

4.1.2 建立健全的民用无人机隐私保护法律

首先,在《民用航空法》中添加针对民用无人机的法律条款,内容应包括民用无人机隐私保护。在上位法的基础上,《民法》《刑法》等法律也需要相应增改条款。各地可针对当地情况出台具体管理规定,将民用无人机管理体系进一步补充完善。另外,由于无人机与其他航空器的差异较大,针对无人机的专门法也应该尽快制定,以规范无人机的使用。

4.1.3 数据安全与数据治理

与民用无人机隐私侵权行为相类似,网络隐私权也包括避免个人受到非法录像监测的地域隐私保护^[18],且民用无人机收集到的个人隐私大概率会被泄露到网络上^[19]。因此,可以通过立法模式对网络隐私权进行保护^[20],将民用无人机隐私侵权添加进相关法律,或是将民用无人机隐私侵权与目前《刑法》中已有的非法利用信息网络罪一起考虑进行修改。在工业级无人机的应用过程中,也要保证与业务无关的数据坚决不采集、不利用,对企业数据治理的过程进行约束,确保其在数据治理框架中完全合法合规。

4.1.4 保障法律发挥实效

首先,需要厘清不同部门对民用无人机的监管职责,避免“无人执法”或“多人执法”的局面^[15]。各部门之间应该实现信息共享,协调推进无人机事务处理。

其次,需要对公民进行民用无人机隐私侵权的普及教育。目前大多数操作者对于无人机隐私侵权的法律观念淡薄,而被侵权者即使意识到个人隐私被侵犯,也会因为不知如何求助处理或认为处理过于困难而放弃维权。所以提高每个公民隐私侵权、维权意识,才能将法律的效力发挥到最大。

4.2 无人机“黑飞”

4.2.1 建立完善的监管系统

“黑飞”问题之所以屡禁不止,没有完善的监管系统是重要原因之一。我国没有具体的处理民用无

人“黑飞”的法律法规,监管主体不明确,行政处罚力度小,警示效果不明显^[21]。为此,首先需要制定针对无人机“黑飞”的监督管理条例,明确无人机“黑飞”的严重性。其次,建立专门的民用无人机飞行管理机构,严格约束民用无人机的飞行,并确保相关条例能落到实处,对违反条例的行为进行严肃查处。

4.2.2 完善现有法律条例

民用无人机飞行管控还需要全面延伸到无人机购买、飞行申请、驾驶执照获取、违法飞行追责方式等环节,使得“黑飞”操作者难以找到监管漏洞。现行民用无人机飞行管控法规多是针对紧急情况制定的,相互之间缺少协调性,甚至出现条款自相矛盾,难以复制推广,使执法难度大增^[9]。所以需要全方位对现有法律条例进行梳理完善,并尽可能出台针对性法律,对民用无人机飞行管控进行全方位整体考虑。

4.2.3 民用无人机实名制与 5G 技术监管

难以对违法无人机追责是我国目前面临“黑飞”问题的一个难点。除微型无人机外,目前我国已经有对无人机进行注册实名制认证的规定。在民用无人机实名制认证的基础上,借助 5G 网络对无人机进行监管,实时监控无人机的位置,方便地进行无人机识别并追责到人,基本解决追责困难的问题。

5 结论

5G 工业无人机作为代表之一,成为在基础设施建设下工业向数字化转型的先驱,需要大力推动其发展。虽然民用无人机使用有一定风险,但该风险可以通过健全的法律法规和完善的监管系统有效控制。我国无人机事业快速发展,但民用无人机法律法规方面的发展较为滞后,尚没有专门的法律条例,对相关问题也缺乏有效法规加以管控。应该对该方面的法律问题加以重视,才能使无人机行业在我国健康良好地发展。

参考文献

- [1] 莫伟,陈颖,覃思旺,等.浅谈 5G+无人机在工业互联网领域的应用[J].广西通信技术,2021(3):19-22.
- [2] 杜斌.5G 助力无人机应用发展 [J]. 信息通信技术与政策,2019(11):8-11.
- [3] 张影.民用无人机侵犯公民隐私安全问题探究[J].

辽宁警察学院学报,2019,21(4):49-53.

- [4] 柳云.民用无人机对他人隐私权的侵害及其规制[D].武汉:华中科技大学,2019.
- [5] 吴文博,唐艳.“5G+无人机”的应用与发展问题研究[J].中国无线电,2021(4):71-72.
- [6] 张凌寒,杜婧.民法典背景下无人机侵害个人隐私的法律规制[J].西北工业大学学报(社会科学版),2020(3):85-92.
- [7] 陶宇.无人机侵权责任法律问题研究 [D]. 广州:广东外语外贸大学,2019.
- [8] 寇佳丽.黑飞不止!谁来监管无人机?[J].经济,2017(10):66-68.
- [9] 李雪.无人机“黑飞”相关法律问题研究[J].宁波广播电视大学学报,2017,15(3):59-64.
- [10] 刘志浩,冯娜.基于民用无人机对公民隐私权侵害的法律规制与保护[J].法制博览,2021(9):129-130.
- [11] 张厚义.民用无人机使用中隐私侵权法律问题研究[D].重庆:西南大学,2020.
- [12] 宋丁博男.民用无人机侵犯公民隐私权的法律规制 [J/OL]. 重庆大学学报(社会科学版):1-17 [2022-01-14].<http://kns.cnki.net/kcms/detail/50.1023.c.20210531.1537.002.html>.
- [13] 刘志浩.民用无人机隐私权侵权责任认定困境与突破[D].长春:长春工业大学,2021.
- [14] 周长军,庞常青.民用无人机隐私侵权行为的法律规制——一个比较法的分析 [J]. 法学论坛,2019,34(6):85-94.
- [15] 张艺.微型无人机侵犯隐私权问题探讨与对策分析[J/OL].中北大学学报(社会科学版),2022(1):71-77 [2022-01-14].<http://kns.cnki.net/kcms/detail/14.1329.c.20220110.1100.024.html>.
- [16] 费丽娅.无人机“黑飞”的社会风险和法律规制[J].铁道警察学院学报,2017,27(6):32-37.
- [17] 胡晨晨.民用无人机下隐私权的民法保护研究[D].兰州:兰州大学,2021.
- [18] 孙锐,赵战生.隐私权“撞击”网络监控[J].信息网络安全,2003(7):25-26.
- [19] 王军.论网络隐私权的保护 [J]. 信息网络安全,2006(4):46-48.
- [20] 周涛裕.刍议网络隐私权的挑战和对策[J].信息网络安全,2008(2):64-67.
- [21] 牡丹.民用无人驾驶航空器黑飞刑事法律问题研

究[J]. 厦门广播电视大学学报, 2018, 21(4): 9-14.

(收稿日期: 2022-01-14)

作者简介:

黄煦淇(2001-), 女, 本科, 主要研究方向: 数据安全法。

洪晟(1981-), 男, 博士, 副教授, 博士生导师, 主要研究方向: 网络信息安全、复杂系统安全运行状态监测与健康管理和复杂系统通用质量“六性”技术。E-mail: shenghong@buaa.edu.cn。

(上接第 25 页)

[10] FIPS. DES Modes of operation[S]. US DOC/NIST, 1980.

[11] LIPMAA H, ROGAWAY P, WAGNER D. Comments to NIST concerning AES modes of operations: CTR-mode encryption[EB/OL]. (2000-09-xx)[2001-03-06]. https://www.cs.ucdavis.edu/~rogaway/papers/ctr.pdf.

[12] BIRYUKOV A, KUSHILEVITZ E. From differential cryptanalysis to ciphertext-only attacks[C]//Proceedings of Advances in Cryptology-CRYPTO'98. Lecture Notes in Computer Science. Springer, 1998: 72-88.

[13] MATSUI M, YAMAGISHI A. A new method for known plaintext attack of FEAL cipher[C]//Advances in Cryptology-EUROCRYPT'92. Lecture Notes in Computer Science. Springer, 1992: 81-91.

[14] BELLARE M, HOANG V T, TESSARO S. Message-recovery attacks on feistel-based format preserving encryption[C]//ACM CCS 16. ACM Press, 2016: 444-445.

[15] MUPHY S. The cryptanalysis of FEAL-4 with 20 chosen plaintexts[J]. Journal of Cryptology, 1990, 2(3): 145-154.

(收稿日期: 2022-04-12)

作者简介:

张玉安(1960-), 男, 博士, 研究员, 主要研究方向: 分组密码、序列密码和 hash 函数设计与分析。

王野(1992-), 女, 硕士研究生, 主要研究方向: 计算数学、金融工程、信息安全。

漆骏锋(1979-), 男, 博士研究生, 主要研究方向: 密码应用、移动安全通信、物联网安全。

(上接第 30 页)

[18] 万方. 个人信息处理中的“同意”与“同意撤回”[J]. 中国法学, 2021(1): 167-188.

[19] 谢钱丰. 大数据时代下计算机网络安全问题及应对方法探讨[J]. 信息网络安全, 2020(S2): 60-62.

[20] 张春艳, 郭岩峰. 大数据技术伦理难题怎么破解[J]. 人民论坛, 2019, 2: 72-73.

[21] LIU J, JUUTI M, LU Y, et al. Oblivious neural network predictions via minionn transformations[C]//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 2017: 619-631.

[22] JUVEKAR C, VAIKUNTANATHAN V, CHANDRAKASAN A. {GAZELLE}: a low latency framework for secure neural net-

work inference [C]//27th {USENIX} Security Symposium ({USENIX} Security 18), 2018: 1651-1669.

[23] MOHASSEL P, ZHANG Y. SecureML: a system for scalable privacy-preserving machine learning [C]//2017 IEEE symposium on security and privacy (SP). IEEE, 2017: 19-38.

(收稿日期: 2022-02-11)

作者简介:

宋青林(2001-), 男, 本科, 主要研究方向: 网络信息安全、大数据安全。

洪晟(1981-), 男, 博士, 副教授, 博士生导师, 主要研究方向: 网络信息安全、复杂系统安全运行状态监测与健康管理和复杂系统通用质量“六性”技术。E-mail: shenghong@buaa.edu.cn。

版权声明

经作者授权，本论文版权和信息网络传播权归属于《信息技术与网络安全》杂志，凡未经本刊书面同意任何机构、组织和个人不得擅自复印、汇编、翻译和进行信息网络传播。未经本刊书面同意，禁止一切互联网论文资源平台非法上传、收录本论文。

截至目前，本论文已经授权被中国期刊全文数据库（CNKI）、万方数据知识服务平台、中文科技期刊数据库（维普网）、JST 日本科技技术振兴机构数据库等数据库全文收录。

对于违反上述禁止行为并违法使用本论文的机构、组织和个人，本刊将采取一切必要法律行动来维护正当权益。

特此声明！

《信息技术与网络安全》编辑部
中国电子信息产业集团有限公司第六研究所