数字时代身份盗窃犯罪的规制与应对*

赵赫栋
(中国地质大学(武汉) 公共管理学院,湖北 武汉 430074)

摘 要:身份盗窃通常是指窃取和使用个人身份以获得经济利益或从事其他犯罪活动的行为,数字时代各国对身份盗窃犯罪的规制将日趋完善。美国通过《防止身份盗窃及假冒法》等联邦立法和州立法,构建起身份盗窃行为独立成罪模式;德国没有专门的身份盗窃犯罪立法,而是在个人信息刑法保护体系中统一规制;英国更重视通过前置法实施严格监管,以降低身份信息泄露、滥用和欺诈的可能性。我国与德国的规制模式类似,但存在忽视个人身份保护、身份盗窃刑法评价不全面以及个人信息保护范围过窄等问题。面对数字时代深度伪造技术的冲击,对身份盗窃犯罪的规制更加捉襟见肘。当前,我国应通过采取个人身份的刑法统一保护模式,将非法使用个人信息行为入刑、扩展个人身份信息的刑法保护范围以及完善身份证件类犯罪规制,建构现有的刑法身份保护体系,加强刑法规定之间的衔接。

关键词:身份盗窃犯罪;个人信息刑法保护;深度伪造
中图分类号:D92;G203 文献标识码:A DOI:10.19358/j.issn.2097-1788.2023.02.009
引用格式:赵赫栋.数字时代身份盗窃犯罪的规制与应对[J].网络安全与数据治理,2023,42(2):53-61,69.

Regulation and response to identity theft in the digital age

Zhao Hedong
(School of Public Administration, China University of Geosciences (Wuhan), Wuhan 430074, China)

Abstract: Identity theft usually refers to the act of stealing and using personal identity to obtain economic benefits or engage in other criminal activities. In the digital age, countries will increasingly regulate identity theft crimes. Through federal legislation such as the Identity Theft and Assumption Deterrence Act of 1998, and state level legislation, the United States has established an independent crime model for identity theft. Germany has no special legislation on identity theft, but unified regulation in the criminal protection system of personal information. The UK pays more attention to strict supervision through the pre law to reduce the possibility of identity information leakage, abuse and fraud. The regulation mode in China is similar to that in Germany, but there are problems such as neglecting the protection of personal identity, incomplete evaluation of criminal law on identity theft, and narrow scope of personal information protection. In the face of the impact of deepfake technology in the digital age, the regulation of identity theft is even more inadequate. At present, China should adopt the unified criminal law protection model of personal identity, improve the existing criminal law identity protection system and strengthen the connection between criminal laws by criminalizing the illegal use of personal information, expanding the criminal law protection scope of personal information, and improving identity document crimes.
Key words: identity theft; criminal law protection of personal information; deepfake

0 引言

身份盗窃通常是指窃取和使用个人身份以获得经济利益或从事其他犯罪活动的行为,早在20世纪90年代末期,美国就正式将身份盗窃犯罪纳入刑法[1]。随着数字时代社会信息化程度的进一步提高,可识别性的身份信息构成个人“数字身份”的核心内容,一旦遭到泄露、盗窃或冒用等不法侵害,对信息主体可能会造成难以弥补的伤害和损失。

作为与计算机信息技术密切相关的犯罪类型,各国未来对身份盗窃犯罪的规制将越来越重视。一是数字身份成为发展趋势。2022年3月10日,英国政府发布了数字身份立法咨询反馈,寻求构建数字

*基金项目:国家社会科学基金重大项目(18ZDA149)

身份立法框架;在我国,2022 年 3 月 25 日,国务院发布《关于加快建设全国统一大市场的意见》,其中“健全统一的社会信用制度”“加快培育统一的技术和数据市场”等举措离不开高效便捷的数字身份。二是生物识别信息技术迅速发展,在加强身份安全的同时也面临深度伪造等技术所带来的更大风险。如何规制身份盗窃犯罪已成为各国所面临的共同法律问题。

美国、德国、英国等信息发达国家的网络犯罪立法较早突破了适用传统犯罪立法的观念限制,设立了独立化、体系化的网络犯罪立法,其立法的成功经验和未来走向对我国具有借鉴价值[2]。本文以美国、德国和英国的身份盗窃犯罪的刑法规定和政策动态为研究对象,对我国刑法中身份盗窃的相关罪名进行梳理,以比较不同立法的特点、优势和不足。

1 欧美身份盗窃犯罪规制模式探析

对身份盗窃犯罪的规制取决于个人信息刑法保护的模式。英国和德国受欧盟的影响,制定有完整的个人信息保护法,在统一的制度框架内规制身份盗窃犯罪。而美国的个人信息保护采用分散立法模式,设有专门的身份盗窃犯罪法。

1.1 美国身份盗窃行为独立成罪模式

作为信息化时代的引领者,美国最早提出“身份盗窃”的概念。2004 年,与金融诈骗交织的身份盗窃犯罪已经是美国“增长最快的犯罪”[1],时至今日,身份盗窃案仍然高居全美诈骗案之首。因此,美国的联邦法和州立法几乎都对身份盗窃犯罪作了规定,不同法律之间存在差异。

1.1.1 联邦立法对身份盗窃犯罪的规定

在联邦层面,两部主要立法《防止身份盗窃及假冒法》和《身份盗窃处罚加重法》的规定存在区别:前者规定“身份盗窃是指未经合法授权,故意转移或使用他人信息,意图实施或参与实施违反联邦法的行为或者所意图实施或参与实施的行为构成州法或地方法上的重罪的行为。”但《身份盗窃处罚加重法》将行为扩展到了“故意转移、拥有或者使用他人信息”。其他如《公平信用报告法》则将身份盗窃限定为“利用他人的身份信息实施的欺诈行为”。有学者对这种犯罪行为的不统一规定提出了质疑,认为忽略犯罪行为不能有效区分不同类型的身份盗窃,提出模仿刑法对传统盗窃罪的区分方式,对身份盗窃犯罪也进行相应区分[3]。

上述身份盗窃犯罪的概念虽没有形成统一意见,但有学者指出身份盗窃犯罪往往由三个阶段的行为组成:第一阶段是非法获取他人身份信息或身份识别凭证;第二阶段是利用盗窃来的身份信息或识别凭证建立虚假身份,即将自己伪装为他人;第三阶段是利用虚假身份获得经济利益或从事其他犯罪活动[4]。总体上,美国刑法规定的身份盗窃罪是故意犯罪,强调特定的犯罪意图,打击犯罪的重点在个人信息犯罪的中下游行为,以上三个阶段的行为完整涵括了一般身份盗窃犯罪。

在刑罚上,美国身份盗窃的刑事责任主要表现为监禁刑和罚金刑。根据《防止身份盗窃及假冒法》规定,身份盗窃犯罪的监禁刑刑期从 1 年到 30 年不等,一般的身份盗窃犯罪可能被判处罚金和 15 年以下的监禁;如果身份盗窃者盗窃身份后实施的行为是贩毒、严重暴力犯罪或之前已经有过本节规定之罪的确定判决,则身份盗窃者可能被判处 20 年以下的监禁;对于支持恐怖主义犯罪的身份盗窃,则会被判处 30 年以下的监禁。罚金刑也是美国对身份盗窃犯罪适用的重要刑罚,美国《身份盗用惩罚措施法》中规定,盗窃他人信件的罚金数额为 2 000 美元;冒用他人身份申请信用卡,可罚款 1 000 美元;如果身份盗窃涉及金融机构,罚款可高达 100 万美元。

1.1.2 州立法对身份盗窃犯罪的规定

州层面对身份盗窃的规定同样各不相同。如华盛顿州规定任何人以犯罪或帮助犯罪为目的,故意获取、持有或者转让他人(不论该人是生是死)的身份或者资金信息的,构成身份盗窃罪;德克萨斯州规定,未经他人同意,基于伤害或欺骗他人的目的,获取、拥有、转移或使用他人的身份信息,构成身份盗窃罪;而亚利桑那州规定,如果行为人以获取或者使用他人或单位的身份信息为目的以便达到任何非法企图,或以获取或者使用他人或单位的身份信息为目的给该他人或单位造成损失,或者以获取或者使用他人或单位的身份信息为目的获取工作或继续工作,在未经该他人或单位的同意下,故意获取、购买、制造、记录、持有或者使用任何有关他人个人身份信息或者单位身份信息(该他人或单位包括真实存在的或者虚构的),成立身份盗窃罪。

州立法在犯罪行为上仍作了不同的概括列举,

且在犯罪对象上也存在区别，如在亚利桑那州法律中“人”不仅包括自然人还包括单位，在华盛顿州则不包括单位，但却包括死者。

在刑罚上，州立法的监禁刑一般更轻。如加利福尼亚州、密西西比州等州刑法都规定身份盗窃罪一般的监禁不超过 1 年，明尼苏达州则根据对被害人造成损失程度的不同设置了最低 90 天，最高 20 年的监禁。上述州立法规定的罚金数额也大都在 1 000 美元至 10 万美元之间[3]。

除了立法上明确规定的监禁刑和罚金刑，法院判例中也存在类似于资格刑的规定，判例中的资格刑并没有统一的模式，而是根据案情的不同情况给予不同的资格限制。如在加利福尼亚州的 People v. Malone 案中，由于被告多次利用他人的身份信息办理信用卡、支票或票据，法院为了使其改过自新并且保护公众的安全，限制被告拥有光电扫描仪和数码相机，并且要求其关闭网络和电子邮件[5]。

1.1.3 未来身份盗窃责任

虽然美国对身份盗窃犯罪给予了较为严厉的刑事制裁，但身份盗窃犯罪始终居高不下。在新冠疫情期间，通过身份盗窃骗取疫情救济金等诈骗案件更是爆发式增长。身份盗窃犯罪的长期困扰促成了“未来身份盗窃责任(Future Identity Theft)”的提出，即从源头上防范，对个人信息的合法拥有者课以严格的责任，不论何种原因个人信息被泄露，其都应对未来的身份盗窃负有责任[3]。

对于这一观点，有法院通过判例表示了支持，如在 McLoughlin v.People′s United Bank 案中，6 到 10 个存储有未加密的个人信息的备份带丢失后，客户们对银行提起了集团诉讼。法院认为，虽根据相关州的债权法并不足以支持诉讼，但是该案中身份盗窃的风险可构成诉权的足够基础。

更多的法院则并不支持扩大身份盗窃犯罪责任。虽然对未来身份盗窃追究责任虽有利于身份盗窃的源头遏制，但是由于其有悖于传统的“现实损害”原则，因此在司法判例中适用仍是少数[3]。

2021 年 4 月 26 日，美国第二巡回法庭在 McMorris v.Carlos Lopez & Associates 案判决中就指出，原告必须证明存在“事实上的损害”，这意味着一种“具体的和特殊的”以及“实际的或即将发生的”的损害，一个“推测的”或“假设的”伤害是不够的。

第二巡回法庭同时提出，理论上原告可以基于身份盗窃的“风险增加”来获得诉权，并据此确定了三个应考虑的因素：(1)数据是否因有针对性地尝试获取而遭到泄露；(2)数据集的任何部分是否已被滥用；(3)已暴露的数据类型是否敏感。在该案中，法庭认为，由于泄露的电子表格中的个人身份信息(PII)高度敏感，原告满足了第三个因素。但他们没有证明 PII 是被公司以外的第三方以窃取等方式故意获得的，不能证明未经授权者使用或滥用 PII，因此不能证明他们面临着未来身份盗窃或欺诈的重大风险。

1.2 德国个人信息刑法统一保护模式

德国没有专门的身份盗窃犯罪立法，而是在个人信息刑法保护的法律体系中统一保护。与美国分散立法不同，德国的个人信息刑法保护是通过附属刑法和核心刑法所建立的二元数据刑法保护模式实现的：一是以《德国联邦数据保护法》(BDSG)中的附属刑法规范为基础，建立对个人数据的全面保护；二是以《德国刑法典》为依托，设立对一般数据的体系保护[6]。

1.2.1《德国联邦数据保护法》

现行的《德国联邦数据保护法》(BDSG)受 2018 年欧盟《通用数据保护条例》的影响，在 2019 年进行了包括刑事犯罪部分在内的大幅度的修订，和欧盟数据保护法对接更为紧密[6]。

(1)内容结构

2019 年《德国联邦数据保护法》共有四个部分，除第一部分共同条款和第四部分补充条款以外，第二部分“为实现欧盟 2016/679 号法规第 2 条之目的的实施条款”、第三部分“为实现欧盟 2016/680 号指令第 1(1)条之目的的实施条款”均对接欧盟的数据保护规定。

欧盟 2016/679 号法规即《通用数据保护条例》，条例第二条规定了一般适用范围，即“适用于全自动个人数据处理、半自动个人数据处理，以及形成或旨在形成用户画像的非自动个人数据处理”。第二条排除了四种不适用的情形，包括“欧盟法管辖之外活动的个人数据处理”“自然人在纯粹个人或家庭活动中的个人数据处理”“欧盟成员国为履行《欧盟基本条约》第二章第五款的个人数据处理”以及“有关主管部门为预防、调查、侦查、起诉刑事犯罪、执行刑事处罚、防范及预防公共安全威胁而进行的个人数据处理”。其中最主要的是政府主管部

门在打击刑事犯罪和预防公共安全威胁过程中的个人数据处理活动,与之相对,第三部分的欧盟2016/680号指令则专门规定主管部门在预防、调查、侦查、起诉刑事犯罪或执行刑事处罚,以及防范和预防公共安全威胁过程中处理个人数据的活动。由此,《德国联邦数据保护法》第二、三部分分别规定普通主体和打击犯罪主管部门的个人数据处理活动。

(2)罪行条款

《德国联邦数据保护法》的罪刑条款主要是第42条,规定:

(1)在未经授权的情况下,以营利的方式故意将多人的非开放个人数据传输给第三方或者通过其他方式使其开放,处3年以下自由刑或罚金刑。

(2)在未经授权的情况下,为了获取报酬,或者为自己或他人谋取利益,或者为了给他人造成损失,包括处理未开放的个人数据或者通过虚假的信息骗取未开放的个人数据,处2年以下自由刑或者罚金刑。

(3)本条刑事犯罪告诉的才处理。有权提出告诉的主体包括数据主体、负责机构、联邦数据保护专员以及监管机构。

该条形成了独立的个人信息犯罪构成要件,行为方式包括传输、公开、处理、骗取,基本涵盖了个人信息犯罪的行为类型。对于身份盗窃犯罪而言,第一款主要规制上游犯罪,即非法获取并转移个人身份信息的行为;第二款规制中下游犯罪,强调为了牟取非法利益或为给他人造成损失而非法处理个人信息的行为。

本条中的处理含义广泛,在2019年修订以前,《德国联邦数据保护法》中个人信息刑法保护行为的类型较为复杂,依前置行政法规范列举了9种违法行为,包括在未经授权的情况下处理、收集、持有、读取个人数据,骗取个人数据,违反相关规定的目的而处理、使用、结合个人数据等;随后规定"为了获取报酬,或者为自己或他人谋取利益,或者为了给他人造成损失",故意实施上述行为的处以2年以下自由刑或罚金刑[6]。新法修订简化了犯罪行为类型,但并没限缩犯罪行为的范围,附属刑法条款构成要件的涵盖面并不狭窄,理论上仍有学者批判性地认为该附属刑法条文具有预防性特征[6]。且刑罚幅度也有所提升,最高刑首次达到了3年以下自由刑。

从立法效果看,简化犯罪行为类型后的刑事条款更加明确,既为合法使用个人信息提供了较宽松的法律空间,也严厉打击为了实施不法活动的使用行为,较好地兼顾了个人信息保护和合法利用两方面的利益。并且作为附属刑法,个人数据保护的刑事条款有完整的前置法规范,《德国联邦数据保护法》详细规定了个人数据处理的情形、数据主体的权利、数据控制者和处理者的义务和监督管理机构等内容,刑事条款的适用更加明确。

1.2.2《德国刑法典》

《德国刑法典》有专门规定个人信息犯罪的第十五章侵害个人生活与秘密领域罪[7],除此以外,第二十三章伪造文书罪、第二十二章诈骗罪、第八章伪造货币与有价证券罪以及第七章妨害公共秩序罪都与身份盗窃行为相关。具体罪名条款和主要内容如表1所示。

与《德国联邦数据保护法》不同,《德国刑法典》第十五章侵害个人生活与秘密领域罪中的数据并非特指个人身份信息,而是指一般的电子数据,即"以电子、磁性或其他无法直接感知之方式存储或传输的数据"[7]。罪名主要集中在数据的非法获取、传输和公开行为,不包括数据的违法使用,涉及的是身份盗窃的上游犯罪,即非法获取个人信息的部分,而非完整的身份盗窃犯罪。因此,第十五章的相关罪名仅处罚行为人出于犯罪或者帮助他人犯罪的目的获取、传输和公开个人信息数据的身份盗窃犯罪。

《德国刑法典》其他章节的身份盗窃犯罪大致可以分为两类,一是盗用、冒用身份、证件等的犯罪;二是身份盗窃的下游犯罪,主要为诈骗罪。涉及盗用、冒用身份、证件等的犯罪主要涉及第二十三章伪造文书罪以及第八章的伪造货币和有价证券罪,也涉及到第七章妨害公共秩序犯罪。在第二十三章伪造文书罪中,第267条伪造文书罪规定,在法律关系中为实施欺诈而制作虚假文书、变造文书,或使用虚假或变造文书的,处5年以下有期徒刑或罚金,情节严重的加重处罚。第270条特别强调,在法律关系中对电子资料的处理产生虚假影响的,视为法律上的欺骗。伪造文书罪中的罪名大都要求行为人主观上有欺诈故意,处罚的范围包括制作、获取、保管、转让和使用伪造、变造文书证件的

表 1 《德国刑法典》中与身份盗窃有关的犯罪

章节	具体罪名	条文内容
第十五章 侵害个人生活与秘密领域罪	第 202a 条窥探数据罪、第 202b 条截获数据罪、第 202c 条窥探和截获数据的预备罪、第 202d 条数据窝赃罪	主要集中在数据的非法获取、传输和公开行为、不包括数据的违法使用
第二十三章 伪造文书罪	第 267 条伪造文书罪第、268 条伪造电子数据罪、第 269 条伪造有证明重要性的电子资料罪、第 275 条伪造官方证明文件预备罪、276 条虚假官方证明文件取得罪、第 281 条滥用证件罪	基本涵盖了通过违法使用他人身份文书、证件实施的身份盗窃犯罪
第八章 伪造货币和有价证券罪	第 152a 条伪造变造信用卡、支票与汇票罪	以欺诈为目的而实施下列行为之一的，处五年以下有期徒刑或罚金：①伪造、变造国内或国外的信用卡、支票、汇票；②为自己或他人取得、贩卖、交付他人或使用此类伪造、变造的卡证、支票或汇票的。该罪规制使用虚假信用卡盗窃他人财务的身份盗窃犯罪
第七章 妨害公共秩序犯罪	第 132a 条冒用头衔、职业与徽章罪	未受准许冒用本国或外国公务人员的职业、学位、头衔或公共荣誉名衔的；冒用医生、牙医、心理治疗师、律师、税务咨询师等职业的；冒用官方聘用人员的；穿戴本国或外国公务人员服饰徽章的，处一年以下有期徒刑或罚金

犯罪行为，刑罚大都在 5 年有期徒刑以下。基本涵盖了通过违法使用他人身份文书、证件实施的身份盗窃犯罪。另外，第八章伪造货币和有价证券罪中的伪造、变造信用卡、支票与汇票罪以及第七章妨害公共秩序犯罪中的第 132a 条冒用头衔、职业与徽章罪也属于身份盗窃犯罪。

其次，诈骗罪等下游犯罪也会涉及身份诈骗。例如《德国刑法典》第 263 条规定“意图为自己或他人谋取不法利益，通过告知虚伪错误事实、或扭曲隐蔽真实事实，引起或维持错误，导致他人财产损害的”是诈骗罪，因此非法使用他人身份信息进行欺诈，意图谋取财产利益的身份盗窃行为也构成诈骗罪。

1.3 英国数字身份事前监管与防范制度

英国也没有对身份盗窃犯罪作出专门规定，而是在包含在《数据保护法案》中。但自 2019 年以来，英国政府正在寻求创建一个数字身份管理框架，该框架能够通过严格的监管和信息共享防范身份滥用和欺诈行为。

1.3.1 《数据保护法案》的轻缓化刑罚设计

《数据保护法案》保护的对象为可以被识别的，与个人相关的数据，其中涉及个人信息犯罪的规定集中在第五章(信息专员)、第六章(执行)、第七章(补充条款和最终条款)以及附件 15 中，共有 13 项罪名。这些罪名的设置围绕着不同的权利、义务采用罪群模式，大致分为四个部分，包括：非法获取、披露、出售、保留个人数据，妨碍执法，侵犯访问权和重新识别去标识化的个人数据，就身份盗窃犯罪而言主要规制的是在上游犯罪行为。

在刑罚设置上，英国 1998 年《数据保护法案》第 60 条规定此类侵犯个人信息犯罪的刑罚仅限于罚金。而过于轻缓化的刑罚不利于对严重侵害个人信息犯罪行为的惩治，导致检方依据其他能够判处监禁的条款起诉成为一种趋势[8]。在修改后的 2018 年《数据保护法案》中，根据第 155~159 条的处罚规定，刑罚仍仅限于罚金，并未配置任何监禁刑。有学者认为采用替代条款起诉严重的个人数据犯罪将仍是英国司法的必然选择。

1.3.2 数字身份保护的严格监管

2022 年 3 月 10 日，英国政府发布了《数字身份立法咨询反馈》(以下简称《立法咨询》)，提出要扩大数字身份在整个经济体中的使用，创建一个数字身份管理框架。在 4 月 6 日发布了更新后的《英国数字身份和属性信任框架 alpha2 版》，该信任框架主要面向数字身份服务的提供者，设立了一系列的义务和责任。

英国的数字身份立法着重从政府和行业监管、身份信息利用的透明度、服务提供者义务、权利救济等方面保护主体的身份信息，主要目的在于构建安全的数字身份制度，促进经济发展。在立法咨询

过程中,由于英国民众普遍表达了对数字身份带来的欺诈、安全风险和侵犯隐私的担忧,因此其更加重视对身份盗窃的防范。

在刑罚方面,和《数据保护法案》相似的是,《立法咨询》仍然采取保守的刑罚政策。第2.6.2.2条指出,《英国通用数据保护条例》和《2018年数据保护法》能够涵盖可能的犯罪行为,因此英国政府不打算设置任何与数字身份有关的新罪行。

在身份安全与防范欺诈方面,《立法咨询》提出应当加强服务提供者、数据主体和监管机构之间的信息共享,以及时发现和预防欺诈和安全事件,从而最大限度地提高安全性并减少欺诈行为。

在政府与行业监管方面,除了政府监管和行业自查,《立法咨询》还通过外部认证评估的方式,由授权的认证机构聘用合格的认证审计师,对服务提供者的安全资质进行专业、持续、严格的把控。

在权利救济方面,基于身份盗窃造成的被害人信誉受损等问题,《立法咨询》专门规定了身份修复,要求服务提供者在出现错误时快速有效地"修复"身份,对个人依法对其数据进行更正和补充的,在一个月内作出回应。

《立法咨询》还在身份信息的收集和使用上规定了最低限度要求,并通过使用属性等概念加以落实,即在某些情况下只进行"是或否"的简单核验,以求最大程度上保护公民身份信息安全。

可见,英国对数字身份保护的规制重心前置,其立法希望通过前置法实施严格监管,降低身份信息泄露、滥用和欺诈的可能性,全面保护数据主体的权益,对于触犯刑法的个人数据犯罪只处以罚金。整体上有重事前监管,轻刑罚处罚的特点。

2 我国刑法对身份盗窃犯罪的规制与面临的挑战

2.1 刑法中的相关法律规定

与德国规制模式相类似,我国刑法中没有规定专门的身份盗窃罪,但有不少罪名涉及了身份盗窃犯罪。对应前述学者将身份盗窃划分的三个阶段,相关罪名可以归纳如下:

第一类是非法获取他人身份信息或身份识别凭证等的犯罪。这一类罪名主要包括:(1)侵害公民个人信息罪,包括违法向他人出售、提供公民个人信息,以及非法获取公民个人信息的行为;(2)妨害信用卡管理罪,其中"使用以虚假的身份证明骗领的信用卡"的规定与身份盗窃直接相关;(3)伪造、变造居民身份证罪,规制伪造、变造、买卖居民身份证、护照、社会保障卡、驾驶证等依法可以用于证明身份证件的行为,以及类似的伪造、变造国家机关公文证件印章罪,伪造公司、企业、事业单位、人民团体印章罪等。

第二类是利用盗窃来的身份信息或识别凭证建立虚假身份的犯罪。这一类的罪名主要包括:(1)使用虚假身份证件、盗用身份证件罪,即在依照国家规定应当提供身份证明的活动中,使用伪造、变造的或者盗用他人的居民身份证、护照、社会保障卡、驾驶证等依法可以用于证明身份的证件;(2)冒名顶替罪,该罪是2020年《刑法修正案(十一)》新增的犯罪,将"盗用、冒用他人身份,顶替他人取得的高等学历教育入学资格、公务员录用资格、就业安置待遇"的行为规定为犯罪。该罪名是对司法实践予以立法回应。2020年6月山东等地陆续曝光陈春秀等多起冒名顶替上大学事件,结合2001年山东齐玉苓案、湖南罗彩霞案,冒名顶替上大学呈现多发态势,引起各方高度重视。该罪名直接规制盗用、冒用他人身份的行为,扩充了个人信息保护的规制行为类型。

第三类利用虚假身份获得经济利益或从事其他犯罪活动,即涉及部分身份盗窃之后续行为的罪名。包括诈骗罪、招摇撞骗罪等。如2020年曹某等人冒充老干妈与腾讯签订合作协议,后被定罪为合同诈骗罪。

在刑罚上,上述等犯罪的最高法定刑大都在七年以下,第一、二类犯罪在我国刑法中大都没有规定罚金的数额,诈骗罪的最高罚金数额为50万元,部分犯罪如招摇撞骗罪规定有资格刑。

2.2 法律规制不足

近年来随着网络的普及,身份盗窃现象始终层出不穷。但由于我国对身份盗窃犯罪的刑法规定分散,没有形成统一的规制体系,在身份盗窃犯罪方面法律规定存在缺失。

首先,重视对实体身份证件的保护,忽视对个人身份的保护。身份盗窃的本质是对身份的盗用。随着信息网络的普及,具有识别性的公民个人信息的地位越来越重要。但目前在数据层面,我国对个人身份的保护主要依靠侵犯公民个人信息罪,而该罪只规制非法出售、提供和获取公民个人信息的行

为,而非身份盗用行为。

其次,刑事法网存在漏洞,如对冒用他人身份承担刑事责任等行为缺乏规制。在行为方式上,除了通过窃用他人身份以违规贷款等方式谋取财产利益,还存在冒用他人身份承担刑事责任的案件。对于冒用他人姓名犯罪的行为人没有合适的罪名加以规制。

最后,刑法中侵犯公民个人信息罪的保护范围也存在不足,尤其是司法解释没有将生物识别信息纳入该罪的保护范围,不利于对身份盗窃犯罪的应对。

综合来看,经过多年的法制改革,刑法上已经规定了多种能够适用身份盗窃的犯罪,但是面对日益严重的身份盗窃,现有的刑法体系还无法应对其所带来的挑战。我国身份盗窃犯罪应首先着眼于完善法律体系的漏洞。

2.3 深度伪造技术的挑战

2.3.1 生物识别信息与深度伪造技术的普及

随着人工智能深度学习算法的进步,“深度伪造”(deepfake)技术应运而生,它是一种基于人工智能深度学习技术产生的新的伪造技术,其主要技术表现是利用人工智能技术实时伪造他人面部表情和声音[9],能让观察者误认为是他人的真实言行的视听记录。

深度伪造技术通过对人类面部、声音、指纹甚至血型、DNA 等信息的综合使用,实现了对个人信息更深层和更全面的掌控。这一技术与身份盗窃紧密相关,在足够的信息支持下,身份盗窃的预防难度和危害性将显著提升。

有学者将深度伪造的本质解读为身份盗窃,这一观点还有待探讨。深度伪造与身份盗窃的区别在于:后者是盗窃冒用他人身份信息,而前者作为一种技术工具或行为方式,并不一定具有身份盗窃的危害性,具体构成何种犯罪,也取决于行为的动机和侵害的法益。只有伪造的身份为不知情的他人时才可能构成身份盗窃,伪造自己的身份(如舞蹈演员将他人的舞蹈动作转移到自己身上)则难以构成犯罪。

身份盗窃犯罪与个人信息犯罪联系密切。近几年来,人脸识别等个人生物识别信息技术以及基于此的深度伪造技术迅速发展,使得身份盗窃可以触及到生物信息这一个人信息的核心,身份盗窃犯罪或将迎来新的发展高峰。

2.3.2 对基于深度伪造的身份盗窃规制存在不足

我国对深度伪造技术的规制主要体现在相关部门发布的法规上。国家互联网信息办公室、文化和旅游部、国家广播电视总局于 2019 年 11 月联合发布的《网络音视频信息服务管理规定》,以及国家互联网信息办公室《网络信息内容生态治理规定》第 23 条都规定相关主体不得利用深度学习、虚拟现实等新技术新应用从事法律、行政法规禁止的活动。《民法典》第 1019 条也规定任何组织或个人不得利用信息技术手段伪造等方式侵害他人的肖象权。

但在刑法上,我国的身份盗窃犯罪规制体系则捉襟见肘:除实体身份证件有关的罪名之外,我国仅有侵犯公民个人信息罪与之直接相关,且缺乏对滥用身份行为的规制。在这一方面我国刑法还有很长的路要走。

美国是对“深度伪造”规制回应最积极的国家,目前有多部法律草案等待国会审议,包括 2018 年《恶意伪造禁令法案》、2019 年《深度伪造报告法案》和《深度伪造责任法案》等,着眼于深度伪造的信息的虚假性,规制深度伪造技术的滥用。例如,《深度伪造责任法案》要求任何利用州际或者国外商业设施及手段制作的深度伪造视频或者明知是深度伪造视频而意图传播的人均应在作品上标记水印。同时法案对三类行为规定了不超过 5 年的刑事处罚,包括:(1)未对作品进行水印标记,且具有羞辱他人的主观目的,提供含他人虚假的性行为或者裸体的视频的;(2)意图造成暴力或者身体伤害、引发武装或者外交冲突,或者干扰政治运作(包括选举),威胁社会信任的;(3)受外国势力或者代理人指示,意图介入国内政治争议,影响联邦、州或者其他的选举,以及实施其他不法行为的。法案还规定了深度伪造的被害人有权采用各种救济措施。

3 完善刑法对个人身份的保护

基于前述对美国、德国和英国身份盗窃犯罪规制模式的分析,结合我国涉及身份盗窃犯罪的刑法规定,本文认为,我国应采取个人信息刑法统一保护模式,无需将身份盗窃行为独立入罪,通过将身份盗窃三个阶段的行为分别定罪,利用罪数规则就可以实现合理的处罚。对个人身份的保护是规制身份盗窃犯罪的核心,在个人身份的刑法保护框架存在漏洞的情况下,需要修改和完善相关的刑法规定。

3.1 个人身份与个人身份信息

身份依赖于社会建构,在多元化的社会,身份制度是维系从传统低流动性的乡土社会到当代高流动性的市场经济社会的相关秩序的基础设施[10]。在数字时代,公民的个人身份已然成为其参与社会活动的重要途径,作为被管理的一方,政府或企业雇主为公民或雇员创建独一无二的身份,在行政管理或劳动管理中加以使用;作为接受服务的一方,互联网平台企业同样为用户创设数字身份用以提供相关服务。可以说,身份附着着个人对人格利益、财产利益和公共利益的多重关切。

首先,对个人身份的保护并不完全等同于对个人信息的保护,由于刑法中"公民个人信息"的概念本身就包含有身份识别性特征,因此任何个人信息都直接或间接地与身份相关联。但并非所有个人信息犯罪都会侵害到个人身份,只有利用非法获取的身份信息建立虚假身份伪装成他人的,才可能构成身份盗窃犯罪。部分个人信息如行踪轨迹信息、通信内容、征信内容、财产信息虽然足以精准识别到公民个人,但行为人只要没有通过冒用身份的方式实施犯罪,就难以认为其侵害了个人身份。因此,对个人身份的保护难以通过单纯提高身份信息本身的保护层级来实现。

其次,在身份信息犯罪与身份盗窃犯罪的关系上,身份信息犯罪往往是冒用身份犯罪的预备行为,能够为身份盗窃犯罪提供必须的作案"工具"[11]。对身份信息犯罪的规制包含于刑法对个人信息的统一保护,在这一点上,我国《刑法修正案(九)》将"出售、非法提供公民个人信息罪"与"非法获取公民个人信息罪"合并为"侵犯公民个人信息罪",提供了总体性、一般性的规制[12]。但对于后续的身份盗窃行为却仍然缺乏关注,这是目前对于身份盗窃行为应当予以刑法规制的根本原因。

3.2 将非法使用个人信息行为入刑

利用盗窃来的身份信息或识别凭证建立虚假身份,实质上就涉及个人身份信息的使用。虽然当前我国刑法没有将此类行为规定为犯罪,但学界和实务界都认识到了非法使用个人信息产生的严重法益侵害性,并尝试提出规制路径,包括在解释论上对非法获取行为进行扩张解释以涵括非法使用[13],在立法论上增设新罪名或者仅在侵犯公民个人信息罪中增设新行为[14]。从立法过程来看,侵犯公民个人信息罪本身就是对"非法出售、提供"和"非法获取"公民个人信息犯罪的整合,未来将"非法利用"行为纳入该罪并新设一款更为合理。

本文认为在侵犯公民个人信息罪中纳入对非法使用个人信息行为的规制,是应对身份盗窃犯罪的关键条款。其一,数字时代塑造身份的技术成本降低,使在各种不同场合通过多元身份进行的活动变得更加普遍,滋生了大量盗用他人信息假冒他人身份的行为。在网络化普及以前,国家机关签发的身份证件、证明文件以及公文印章是认定身份的主要依据,国家身份证件等的管理制度是身份保护的核心;而当前仅凭身份信息本身就足以实现牟取利益、侵害他人的目的,甚至利用盗用的信息就可以注册国家机关的证明文件。近年来此类案件层出不穷,尤其随着生物识别技术普及,非法使用身份信息的行为在身份盗窃犯罪中将扮演重要角色。其二,非法使用个人信息行为入罪能够使身份盗窃犯罪得到更加完整的评价。一般来说,行为人盗用身份是为了实施获取利益或者侵害他人的行为,当情节严重构成犯罪时,往往以后一行为触犯的罪名处罚而忽略对盗用他人身份的行为的处罚。如果行为人没有实施后续性犯罪行为,或者说没有证据能够证明行为人将要实施后续性的犯罪行为的话,则根本无法进行刑法评价。此时,盗窃个人身份的行为无论多么严重都完全游离于刑法打击半径之外,导致被害人的合法权益无法得到有效的刑法救济[11]。非法使用个人信息行为入罪则可以解决这一问题,无论行为人是否实施后续犯罪行为都能够加以规制。并且根据身份盗窃行为与后续犯罪的关系,行为人可能被判处数罪或者根据想象竞合判处一罪,但即使以后续罪名定罪,仍然可以提醒审判人员注意身份盗窃的事实从而周延刑法的评价。

3.3 扩展个人身份信息的刑法保护范围

我国刑法未对侵犯公民个人信息罪中的个人信息范围作限定,但根据2017年最高人民法院和最高人民检察院联合发布的《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》(以下简称《解释》)的规定,公民个人信息是指"以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息,包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹

等”。同时《解释》第5条第1款还根据受侵害信息类型的不同将其划分为三个层级并设置了高低有别的入罪门槛,实现了对公民个人信息的分级保护[12],如表2所示。

由表2可以看出,我国刑法对个人信息的分级保护大体上是合理的,但也存在一些问题。首先,第一层级的保护范围过窄,应当将生物识别信息纳入其中。其一,生物识别信息的滥用具有危害性大、持续时间长、难以弥补修复以及影响难以根除等特点[15],生物识别信息应用广泛,由此盗用的身份可用于智能支付、门禁安防、交通出行、金融认证、出入境管理等。其二,生物识别信息已经得到越来越多的国家关注和重点保护,美国《防止身份盗窃及假冒法》中规定的“他人身份证明材料”明确包含了“独有的生物识别特征,如指纹、声纹、视网膜或虹膜图像,或其他独有的物理图像”;欧盟GDPR将基因数据、生物识别数据作为特殊数据严格限制处理;我国2020年颁布的《个人信息安全规范》也列举了面部特征、指纹、声纹等七种生物识别信息。因此,生物识别信息高度敏感、具有唯一性和不可变更性,应当作为第一层级的信息受到刑法保护。

其次,第二层级的认定标准不全面,应当合理扩张。第二层级将认定标准限定为“影响人身、财产安全”,而该项所列举的“健康生理信息”也仅指显示健康状况的个人信息。这就将涉及人格、隐私、名誉等的身份盗窃排除在外,相关的信息类型则只能被划入第三层级,入罪标准的适用要求最高,明显不利于刑法对身份盗窃犯罪的规制。因此,可以将标准扩张为“影响人身权利、财产安全”以周延对个人身份的保护。

3.4 完善身份证件类犯罪

2022年2月,国务院办公厅印发《关于加快推进电子证照扩大应用领域和全国互通互认的意见》,明确指出到2025年电子证照应用制度规则更加健全,应用领域更加广泛。其中推广居民身份证电子证照应用是建设数字中国、提高政务服务能力的重要举措。近年来,各地各行业大力推动电子身份证,在金融、教育、医疗、社保、税务等多种业务场景中广泛应用。

电子身份证是身份证件的电子化,包括身份证照面信息、证照文件和证件识别码等内容,仍由公安机关进行认证。由此产生的问题是,我国刑法中规定的伪造、变造居民身份证罪、使用虚假身份证件、盗用身份证件罪的客体是否包括电子身份证及其他电子身份证件?电子身份证件是否属于侵犯公民个人信息罪中的个人信息?

本文认为电子身份证件除具有个人身份信息的属性,还承载着国家机关对于“身份证件”的专有制作、颁发权,目前的电子身份证由公安机关认证,政府各部门在办理业务时对照审查,其与传统实体身份证的签发和使用一致,可以认定为刑法中的居民身份证。但一方面,需要通过立法或者司法解释的途径将电子身份证件明确纳入身份证件类犯罪的范围,以贯彻罪行法定原则;另一方面,根据身份证件犯罪的保护法益,也应限定电子身份证件的具体种类,规定由政府机构签发,由政府统一管理或授权管理。

4 结论

习近平总书记在全国网络安全和信息化工作会议上强调,“没有网络安全就没有国家安全,就没有经济社会的稳定运行,广大人民群众利益也难以得到保障”。对身份盗窃犯罪的规制和应对无疑是涉及人民群众切身利益的网络安全的关键环节。在本质上,身份盗窃犯罪实质上是对身份的滥用,在当前尤其表现为对数字身份的滥用,因此刑法对身份盗窃犯罪的规制实际上是对个人身份包括数字身份的保护。刑法保护数字身份的重要性无需赘言,但采取何种方式进行保护则是数字时代各国刑法必须思考的重要问题。本文基于对美国、德国和

表2 我国刑法对公民个人信息保护的三层级

保护层级	保护范围	入罪标准(情节严重)	开放/封闭
第一层级	行踪轨迹信息、通信内容、征信信息、财产信息	非法获取、出售或者提供50条以上	封闭式列举
第二层级	住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的公民个人信息	非法获取、出售或者提供500条以上	开放式列举
第三层级	第一、第二层级以外的公民个人信息	非法获取、出售或者提供5 000条以上	兜底式规定

(下转第69页)

电,2021,50(12):51-58.
[16] 钱来,王伟.一种基于C-GRU飞行轨迹预测方法[J].电子测量技术,2022,45(10):87-92.
[17] 许阅,刘光杰.基于注意力机制的Bi-GRU内容流行度预测算法[J].电子测量技术,2022,45(3):54-60.
[18] KENNEDY J,EBERHART R.Particle swarm optimization[C]//Proceedings of the 1995 International Conference on Neural Networks.Piscataway:IEEE,1995:1942-1948.
[19] 范伟,孟江,杜永飞,等.基于改进粒子群算法的精密隔振系统LQR控制[J].电子测量技术,2022,45(2):104-109.
[20] 申洪涛,岳凡丁,史轮,等.考虑DG及负荷时序性的多目标配电网重构与DG调控综合优化规划[J].现代力,2022,39(2):182-194.
[21] 郝少伟,李勇军,赵尚弘,等.基于改进粒子群算法的多载波NOMA功率分配策略[J].电子学报,2020,48(10):2009-2016.
[22] 邢海燕,王松弘泽,弋鸣,等.基于IPSO-GRU深度学习算法的海底管道缺陷尺寸磁记忆定量反演模型[J].工程科学学报,2022,44(5):911-919.
[23] 李兴华,牛拥军,雷鸣,等.火电机组脱硫系统超低排放改造节能优化[J].热力发电,2017,46(11):119-123.
[24] 陆晨旭,高海东,高林,等.基于粒子群算法的模糊控制器设计及其在烟气脱硝中的应用[J/OL].热力发电,2022(4):188-193[2022-04-24].

(收稿日期:2022-11-29)

作者简介:
杨兆祥(1995-),男,硕士研究生,主要研究方向:先进控制策略在大型火电机组的应用、机器学习等。
金秀章(1969-),男,博士,副教授,主要研究方向:先进控制策略在大型火电机组的应用、信息融合技术等。

(上接第61页)

英国身份盗窃犯罪规制模式的分析,结合我国涉及身份盗窃犯罪的刑法规定,提出以完善现有刑法身份保护体系,加强刑法规定之间的衔接为主要内容的设想,以供思考。

参考文献

[1] 亨利·庞特,彭新林,高晴.身份盗窃:有限理性、研究与对策[J].刑法论丛,2018,56(4):594-603.
[2] 皮勇.中美网络犯罪立法比较及给我国的借鉴[J].社会科学辑刊,2021(5):123-134.
[3] 马改然.美国身份盗窃的最新发展趋势[J].学术论坛,2012,35(5):50-55,62.
[4] GORDON G R,WILLOX N A,D J R.Identity fraud:a critical national and global threat[J].Journal of Economic Crime Man Agement,2004(2):1-47.
[5] PARKER L J.Validity,construction,and application of state statutes relating to offense of identity theft[J].American Law Reports ALR5th.
[6] 王华伟.数据刑法保护的比较考察与体系建构[J].比较法研究,2021(5):135-151.
[7] 何赖杰等.德国刑法典[M].台湾:元照出版社,2019.
[8] 陈梦寻.中英个人信息犯罪比较研究[J].重庆邮电大学学报(社会科学版),2019,31(6):40-48.
[9] 李怀胜.滥用个人生物识别信息的刑事制裁思路——以人工智能"深度伪造"为例[J].政法论坛,2020,38(4):144-154.
[10] 王立梅,郭旨龙.网络法学研究[M].北京:中国政法大学出版社,2022.
[11] 于志刚.关于"身份盗窃"行为的入罪化思考[J].北京联合大学学报(人文社会科学版),2011,9(1):77-87.
[12] 黄陈辰.侵犯公民个人信息罪"情节严重"中信息分级保护的结构重塑[J].东北大学学报(社会科学版),2022,24(1):95-103.
[13] 李振林.非法取得或利用人脸识别信息行为刑法规制论[J].苏州大学学报(哲学社会科学版),2022,43(1):72-83.
[14] 卢勤,张宜培.非法使用个人信息行为入刑的立法构思[J].河北法学,2023,41(1):73-96.
[15] 程啸.为个人生物识别信息打造法律保护盾[J].人民论坛,2020(24):118-120.

(收稿日期:2023-01-20)

作者简介:
赵赫栋(1997-),男,硕士研究生,主要研究方向:网络安全法学、刑法学。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部