

共享文档信息整合中的刑事风险与刑法应对

黄陈辰

(中央民族大学法学院,北京 100081)

摘要:相对于传统本地文档而言,以实时协同为主要特征的共享文档更有利于提高信息整合效率,保障信息内容即时更新,但其亦为侵犯公民个人信息类犯罪提供滋生的土壤,导致犯罪手段升级、犯罪场景新增、涉案信息数量更大、信息流转范围更广等问题。此类刑事风险对公民个人信息权益及与之关联的人身、财产权益造成严重威胁,亟需刑法予以应对。共享文档信息整合过程中涉及文档创建者、转发者、填写者、修改者、副本制作者、持有者等多方主体,各主体扮演的角色不同,具体行为方式也存在差异,因而应基于类型化思维,针对不同主体的典型行为类型分别进行考量,判断该行为是否符合侵犯公民个人信息罪之行为要件,以确定具体的刑法规制进路。涉案信息数量的大小对于行为人罪与非罪的判断与刑罚轻重的裁量至关重要,在进行数量认定时,不仅应关注一般认定规则,还应考量由共享文档多人协同编辑、内容实时更新等特性所导致的特殊情形的处理。

关键词:共享文档;刑事风险;侵犯公民个人信息罪;公开信息;数量认定

中图分类号:D 924.3

文献标识码:A

文章编号:1000-260X(2023)05-0097-10

互联网时代,随着大数据、云计算等前沿科技的发展以及社会公众对碎片化信息汇集整理需求的提升,越来越多的智能工具、产品与服务开始走向“云端”,例如云储存、云物联等,以及近年来在协同办公、医疗救助等领域发挥重要作用的共享文档即是其中典例。所谓共享文档,指的是支持多人多端协同编辑,实时呈现最新内容,有效实现跨地域、跨组织、跨部门信息整合^①的新型集中式电子文档。区别于传统本地文档低效的传输汇总,其通过“文档上云”能够简化不同主体之间的协作方式,不仅大幅提高信息整合效率,而且能够保障信息内容的即时更新。凭借其协同性、实时性、集成性特征,共享文档在众多场景得到广泛运用,例如在线办公、实时社区、共同创作等。

相对于传统本地文档而言,以实时协同为主要特征的共享文档在信息收集汇总方面具有得天独厚的优势。然而,技术进步在为经济发展、生活便利等提供助力与增益的同时,风险也随之而来。由于共享文档支持多人多端协同编辑,因此信息供给方广泛且不特定,在信息整合过程中易为侵犯公民个人信息类违法犯罪行为的滋生提供土壤。例如在“渣男登记表”事件中,包含姓名、手机号码、家庭住址、照片在内的大量个人信息由于被他人擅自输入共享文档而遭到泄露。另外,共享文档的特性使得上述违法犯罪行为与传统非法提供、非法获取公民个人信息行为不同,对其的认定与规制亦更加复杂,两者无法直接比照。正因如此,探讨共享文档信息整合中的刑事风险及其刑法应对,对于打击相

收稿日期:2023-08-31

基金项目:国家社科基金青年项目“个人信息有序共享的刑民一体化保护研究”(20CFX027)

作者简介:黄陈辰,法学博士,中央民族大学法学院讲师、师资博士后,主要从事刑法学、数据法学研究。

关犯罪、有效保护公民个人信息权益具有重要的理论意义与现实价值。

当前,学术界尚不存在针对共享文档信息整合中刑事风险及其刑法应对的专门研究,虽已有部分论著开始关注医疗、政务等领域内相关信息的共享及其风险防治^[12],但其探讨的重点在于信息共享本身,而非通过共享文档进行信息整合。有鉴于此,本文拟通过梳理分析共享文档信息整合过程中所产生的刑事风险,结合《刑法》第253条之一“侵犯公民个人信息罪”的具体内容,对刑法如何合理应对该类风险提出针对性建议,以期有效规制相关行为,实现对公民个人信息的周全保护。

一、共享文档信息整合中的刑事风险

科技进步在促进经济发展、改善社会生活的同时也不可避免地增加了社会的风险^[13]。虽然共享文档使得信息整合更加便捷、高效,但其使用过程中的刑事风险也开始逐步显现。这些风险主要集中于对公民个人信息的侵犯,但也包含网络谣言、平台责任等其他方面。

(一) 延展犯罪危害性之广度: 犯罪手段升级与犯罪场景新增

近年来,随着公民个人信息内在价值的显现,对信息权益的侵犯亦愈演愈烈,相关案件层出不穷,案件数量逐年攀升^[14]。虽然已有学者开始呼吁应将非法利用公民个人信息行为纳入刑法规制范围,但当前侵犯公民个人信息的最主要方式仍为非法获取与非法提供,集中于个人信息的流转环节^[15]。共享文档的便捷性特点使其容易成为侵犯公民个人信息犯罪的新型工具,行为人可以通过创建共享文档并发送给他人填写的方式,大规模收集公民个人信息,填写者也能够将其所掌握的个人信息同时共享给其他所有接收到该文档的主体。相较于利用传统本地文档实施侵犯公民个人信息犯罪而言,共享文档大幅提升了犯罪效率。需要注意的是,犯罪手段的升级虽然并没有突破传统犯罪行为类型或形塑新的行为模式,仍然表现为非法获取与非法提

供,但其很大程度上拓宽了二者的具体外延,增加了新的犯罪场景。在使用传统手段非法获取公民个人信息时,行为人的目标对象通常为某一主体所掌握的大量信息,例如黑客侵入某银行数据库窃取海量用户信息。此时信息持有者相对单一,由于犯罪成本过高、缺乏可操作性等原因,极少会出现行为人同时针对多个仅掌握少量信息的主体实施窃取行为的情形。但当共享文档被运用到侵犯公民个人信息犯罪中后,行为人对信息持有者所掌握的信息数量不会再有过高的要求,即使信息密度极低,其也能通过共享文档多人多端协同编辑的特性将众多主体所掌握的少量信息汇聚起来。另外,根据最高人民法院、最高人民检察院《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》)第4条的规定,购买、收受、交换等均属于侵犯公民个人信息罪中的“以其他方法非法获取”,其中交换行为通常表现为“一对一”的模式。对于传统本地文档而言,几乎不存在“一对多”或“多对多”交换的情形,但在完全开放的共享文档中,由于文档接触者均可填写并查阅文档内的全部信息,因此形成了一个实质意义上的信息集散中心,各行为人均能够利用共享文档进行信息交换,是典型的“多对多”模式,极大地提升了交换效率。

(二) 加重犯罪危害性之深度: 涉案信息数量大且流转范围广

行为人利用共享文档侵犯公民个人信息的表现形式无外乎非法获取与非法提供两类,虽仍属于侵犯公民个人信息罪的典型行为类型,但由于共享文档实时协同的特性,使得相较于利用传统本地文档而言,前者的危害性程度更深,对法益的侵害更加严重。首先,随着信息时代的到来,侵犯公民个人信息的案件数量快速增长^[16],这些案件中非法获取或非法提供公民个人信息的行为主体较为单一,涉案信息数量完全取决于该主体所掌握的信息规模,虽然也存在海量信息泄露的情形,但具有一定的偶然性。若将共享文档运用于相关犯罪,则所有能够接触到该文档的主体均可以将自身所掌握的个人信息批量填入其中,也可以从中获取他人上传的信息,因此相对于传统情形而言,个人信息的

来源更加广泛,涉案信息数量更为庞大,并且随着共享文档传播范围的延伸,参与主体不断增加,所侵犯的公民个人信息数量将呈指数型增长。其次,对于传统的侵犯公民个人信息行为,通常行为人仅实施非法获取或非法提供行为之一,只有少部分场合才会出现行为人同时实施两种行为的情形,且一般表现为非法获取后又提供,针对的是同一批个人信息。共享文档在允许所有接触者访问其内容的同时还赋予后者编辑的权利,因此大多数情况下文档接触者既提供信息也从中获取信息,致使涉案信息数量成倍增长,犯罪危害性程度也不断加深。再次,在传统情形中,无论涉案信息规模多大,其都是一个固定值,因此信息数量的认定相对容易。而共享文档允许多人多端协同编辑,文档接触者不仅可以填写,还能够进行修改、删除等操作,因此其中所记载的信息数量呈现出浮动样态,进而导致信息数量难以准确认定,影响侵犯公民个人信息罪的合理适用。最后,传统情形中已存在利用网络公开个人信息,从而导致传播范围广泛的案例,如“华住开房记录泄露案”中黑客在网上出售用户在华住官网注册的资料、顾客的酒店入住登记信息等,其中部分信息作为样品被直接公开⁷⁴。需要注意的是,传统情形中虽个人信息被公布于互联网之上,但并非所有人都能注意到并获取每一条被公开的信息,而在利用共享文档实施相关犯罪的情形中,但凡已经填入的信息,对于任何持有该文档的主体而言都是处于被获取的状态。同时,传统情形中若信息发布者再次发布其他个人信息,他人只要未持续关注或刻意查询,则无法及时获知,而共享文档中的内容实时更新,因此所有文档接触者均能零时差地获取他人发布的所有个人信息,导致被侵害的公民个人信息流转范围更广,对信息权益的损害也更深。

(三)其他方面的刑事风险

其一,网络谣言与网络暴力。互联网的虚拟性与匿名性在增加公众利用信息网络发布不实、不当言论风险的同时,还进一步扩大并强化了“法不责众”的心理,导致近年来涉及网络谣言、网络暴力的不良事件频频发生⁷⁵。在利用共享文档进行信息整合的过程中,部分文档接触者出于各种目的可能在

文档中填写虚假信息,该行为虽然并不侵犯相关主体的信息权益,但对其名誉、隐私、正常生活秩序亦会造成极大的危害。其二,共享文档依赖于网络,这是其与传统本地文档的核心区别,共享文档也因此成为互联网公司或平台的运营业务之一,例如腾讯文档、金山文档、石墨文档等。网络技术的发展在便利社会生活的同时亦带来相应风险,随着互联网产品及服务的普及,网络脱序行为、违法行为甚至犯罪行为不断出现,严重危害公民合法权益。在此背景之下,《民法典》《网络安全法》《个人信息保护法》等法律法规对网络服务提供者的安全管理义务提出了明确要求。因此在涉及利用共享文档侵犯公民个人信息、散布网络谣言、实施网络暴力的情形中,不仅行为人可能涉嫌相关犯罪,网络服务提供者若不履行法律、行政法规规定的义务,亦可能构成《刑法》第286条之一“拒不履行信息网络安全管理义务罪”。

二、共享文档信息整合中相关主体行为的刑法规制

由于共享文档信息整合可能导致前述刑事风险,并严重侵犯公民个人信息自决权及其他合法权益,因此刑法必须针对性地对其予以回应。共享文档信息整合过程中涉及多方主体,主要包括文档创建者、转发者、填写者、修改者、副本制作者、持有者等,各主体扮演角色不同,具体行为方式存在差异,刑法对其的规制也必然应有所区别,因此本文基于类型化思维,分别对不同主体行为的刑法规制进路进行具体的分析与研究。

由于所有共享文档接触者均能访问其中的内容,因此文档中所记载的个人信息相对于文档接触者而言属于公开信息,尤其是在该文档不设任何权限时,其中的个人信息更是属于实质意义上的公开信息。对于获取、提供公开信息行为的刑法规制问题,学界已有不少研究,主流观点认为刑法对公开信息与非公开信息的保护力度须有不同,应以“合理处理”作为未经许可获取、提供公开信息的出罪事由⁷⁶,这一观点也得到《民法典》第1036条与《个人信息保护法》第27条的印证。但无论是学界

观点还是法律规定,处理公开信息行为的出罪事由均聚焦于信息主体自行公开或者其他已经合法公开的信息,若个人信息被他人非法公开,则仍应受到类似非公开信息的保护^[1]。在共享文档信息整合过程中,填写者合法或非法将他人信息记载入文档的情形同时存在且以后者为主,因此本文以非法公开个人信息为主要情形对相关行为的刑法规制路径进行研究,仅在涉及合法公开的场合时对信息处理行为是否合理进行判断。

(一) 创建者行为的刑法规制

创建者指的是运用相关程序制作共享文档的主体,其决定了共享文档信息整合的主题并能够设置该文档的可视范围与编辑权限,是信息整合行为链条的起点与源头。创建者基于某种信息整合目的制作共享文档的行为本身并非侵犯公民个人信息的实行行为,不会对作为该罪法益的信息自决权造成直接侵害,但其实质意义上为之后非法获取、非法提供行为的实施准备了工具,制造了便利条件,因此看似可能构成该罪的预备犯。但需要注意的是,若创建者制作共享文档之后继续着手实施其他行为,则由于二者之间存在的阶段性发展关系,前行为被后行为吸收,不再单独被评价为犯罪预备^[2];若创建者制作共享文档后由于各种原因未能继续实施其他行为,由于侵犯公民个人信息的入罪门槛为“情节严重”,并且《解释》第5条第1款对其内容进行了明确界定,包括信息用途及流向、信息类型及数量、违法所得等在内的任何情形,都要求行为人均已着手实施,因此创建者此时不满足“情节严重”的要求而不构成预备犯。总而言之,创建者的创建行为本身不构成犯罪。创建者本身也可能实施转发、填写、修改、副本制作、持有等行为,对其的规制按照相应主体的行为处理即可,此处仅论述创建者最典型的行为类型,后文论述其他主体行为的刑法规制亦是如此。

(二) 转发者行为的刑法规制

转发者指的是将已经制作完毕的共享文档发送给他人的主体。为进行信息整合并扩大信息收集与传播半径,转发者必然会将已经存在的共享文

档发送给其他主体。首先,若共享文档中尚未记录任何信息,则转发者转发空白文档的行为不应被认定为侵犯公民个人信息罪中的提供行为,即使事后有主体在文档中填写他人个人信息进而使得文档接收者通过该文档获取相关信息,转发者也只是提供了信息集散的“场地”或“平台”,而并没有提供信息本身。其次,若共享文档已记录有个人信息,则转发行为属于侵犯公民个人信息罪中的提供行为,涉案信息数量按转发时文档中已存在的信息进行认定。再次,无论转发时共享文档中是否已有个人信息,转发行为均使得接收者能够接触并访问该文档,进而能够在该文档中填写信息或者获取文档中所记录的他人填写的信息,因此转发行为为他人获取、提供公民个人信息的行为提供了帮助,并且具有帮助故意,故在满足其他条件的情况下可构成侵犯公民个人信息罪的帮助犯。最后,在部分情况下,转发者将文档转发给他人后会明确要求他人填写,此时转发者实质上是在积极主动地收集个人信息,且主观上具有收集故意,因此应被认定为侵犯公民个人信息罪中的获取行为。

(三) 填写者行为的刑法规制

填写者指的是向共享文档中填入相关信息的主体,其是共享文档信息整合过程中的信息来源。之所以共享文档能够打破信息孤岛,形成庞大的信息数据库,极大程度上依赖于填写者的信息输入,众多填写者将其所掌握的不同数量的信息填进共享文档,使得文档中的信息数量得以呈指数型增长。

填写者在共享文档中填写相关信息的行为是共享文档信息整合的核心步骤。与转发行为不同,填写行为并非只是提供信息集散“平台”,而是实实在在地提供信息本身,因此应当被认定为侵犯公民个人信息罪中的提供行为。填写者在共享文档中输入个人信息的行为既可能具有合法性基础,也可能本身即为非法,前者如疫情期间民间自发形成的“互助文档”,求助者自愿将其姓名、住址、联系方式等信息登记于共享表格^[3],后者如前述“渣男登记表”,是行为人未经本人同意擅自将其信息曝光。在填写行为非法的情况下,不影响填写者及其他主体行为的判断,但若填写行为合法时,则在部分情形

中,对行为的认定与规制会有变化。行为人合法在共享文档中填写相关信息,其填写行为本身不构成犯罪,但所带来的直接影响是存在于共享文档中的此部分信息即成为他人自行公开或者其他已经合法公开的信息。根据《民法典》第1036条与《个人信息保护法》第27条的规定,其他主体对于此部分信息的获取、提供行为是否合法,取决于其行为方式是否合理。若相关行为符合信息主体的自身意愿或强制公开目的时,则属于合理处理,因此行为合法^[4],例如行为人将“互助文档”转发给他人,虽未经求助者许可,但符合其希望该信息广泛流转的目的,因此不应被认定为非法提供;若相关行为不合理,例如将“互助文档”中的信息提供给犯罪分子,后者利用这些信息实施电信诈骗等违法犯罪行为,此时虽然文档中信息已经被公开,但由于提供行为不符合信息主体之意愿,因此不具有合理性,应属于非法提供。需要注意的是,由于共享文档所具有的实时性特征,填写者将其所掌握的个人信息填入文档时,其他文档接触者即可立刻获知该信息的全部内容,亦可对该信息加以利用,因此填写者的填写行为本身即构成对个人信息的提供,无需其将文档传输或发送给其他人。至于填写行为提供信息的接收方,应指的是能够接触并查看文档内容的全部主体,不仅包括填写行为发生时已经持有该文档的主体,而且包括未来可能持有该文档的主体,因为其在获得共享文档时即能够获知文档中所记录的全部信息内容。

(四)修改者行为的刑法规制

修改者指的是对共享文档中的信息内容进行增补、删除、改动的主体。由于共享文档支持多人多端协同编辑,对于他人输入的信息,行为人可以进行修改,修改后的内容会实时更新在文档之中。修改行为包括增补、删除与改动。增补实质意义上即为填写行为,在实施增补时,修改者实则扮演填写者的角色,其行为的刑法规制参照填写者部分即可;删除是将他人填写的信息从文档中抹掉,在信息由他人非法提供的场合该行为不具有非法性,而在信息由他人合法提供的场合则可能涉及寻衅滋事类犯罪,并会对信息主体的信息权益造成损害。

本文此处主要讨论的是修改者的改动行为,即将他人填入共享文档的个人信息内容进行修改,例如修改姓名、工作单位、联系方式等。虽然《民法典》《个人信息保护法》《网络安全法》所规定的个人信息处理行为包括收集、存储、使用、加工、篡改等,但侵犯公民个人信息罪的行为类型仅有非法获取与非法提供^[5],因此修改者的改动行为本身不构成犯罪。修改者改动共享文档中的个人信息将会导致其真实性发生变化,根据变化的具体情况,可以分为3种情形。其一,修改者将文档中真实的个人信息改为虚假信息,此时改动行为未侵犯他人信息权益或其他合法权益,不具有非法性,但若行为人将他人合法填写的信息,例如“互助文档”中的信息恶意修改,致使他人需求无法实现,严重扰乱社会秩序的,可能构成寻衅滋事类犯罪。其二,修改者对文档中虚假的个人信息进行修改,改动之后的信息仍然是虚假信息,该行为不具有非法性。其三,修改者将文档中虚假的个人信息改为真实信息,这一改动行为实则属于填写行为,需按照填写行为的规制路径处理。

(五)副本制作者行为的刑法规制

副本制作者指的是制作某共享文档副本的主体。在共享文档之外制作一个内容与之相同的本地文档的意义在于其能够将某一时间节点的文档内容固定保存下来,防止他人修改、编辑或因其他原因而无法访问,更方便行为人对其中的个人信息进行利用。副本制作行为本身并不是信息获取行为,不构成侵犯公民个人信息罪,因为在行为人持有共享文档时即已经获知其中的信息内容,制作副本只是将相关信息换一种形式呈现出来,变换的是其载体,信息内容完全一致。在得到共享文档副本后,若行为人又将其传播给他人,则相当于传播本地表格,至于该行为是否具有违法性则需要考察原共享表格的访问权限范围。若原共享表格针对所有主体公开,则副本对于所有人而言均属于公开信息,行为人的传播行为是否违法需根据填写人是否合法提供信息以及传播方式是否合理来确定;若原共享表格仅针对部分主体公开,则在相关主体内传播副本的行为与前一情形相同,但若将副本传播至

相关主体范围外,则属于擅自传播非公开信息,具有违法性。另外需要注意的是,由于共享文档的实时性特征,其中的信息内容时刻发生着变化,甚至由于权限等原因可能导致某一时间段后信息无法访问,因此对相关主体提供、获取个人信息的范围及数量进行认定相较于本地文档而言更为困难与复杂,而副本固定保留了共享文档某一时间节点的历史版本,使得其能够发挥另一重要作用,即成为佐证前述内容的重要证据,有利于司法机关进行行为性质的认定与定罪量刑。

(六)持有者行为的刑法规制

持有者指的是能够接触共享文档并访问其内容的主体。持有者对共享文档及所载个人信息的获取可以分为主动与被动两种形式,若其积极索取,主动要求他人将共享文档发送给自己或明确希望他人向其中填写信息,那么持有者的行为应当属于侵犯公民个人信息罪中的“获取”;若其没有明确表示索取,只是接收了他人转发给自己的共享文档,则其持有行为属于被动收受。被动收受是收受行为的一种,属于《刑法》第253条之一中的“其他方法”,但至于其是否构成犯罪,本文认为应结合主观目的进行分析。具体而言,若收受方具有非法获取公民个人信息的主观目的,则在满足其他要件的情况下应认定其构成侵犯公民个人信息罪;若收受方不具有前述主观目的,甚至对于自己被动接受到公民个人信息的情况毫不知情,则应当阻却犯罪的成立。因此对于被动收受行为的判断取决于行为人的主观目的,而并非部分学者所提出的以行为之主动与否为标准^[6],被动收受行为不必然出罪。

上文分别对不同主体相关行为的刑法规制路径进行了具体的分析,除此之外,还有以下两方面的内容需要特别注意。

其一,从上述内容来看,各行为人均存在多种行为类型,这些行为类型又被认定为对应于侵犯公民个人信息罪的不同行为方式,虽看似繁杂,但其中不少行为呈现出一体多面的样态,其实质上属于同一行为的不同表现形式,因此按一罪名认定即可,只有在数量认定与刑罚裁量时才予以特殊考量。例如在创建者第一次转发共享文档并要求他人填

写相关信息的场合,其转发行为不仅为他人获取与提供个人信息提供了帮助,同时亦属于获取个人信息的实行行为,但由于创建者仅实施了一个行为,因此认定为侵犯公民个人信息罪一罪即可,避免对其重复评价。即使并非同一行为,而是行为人确实实实在实施了帮助行为,又实施了获取行为或提供行为,但由于其均属于侵犯公民个人信息罪的行为方式,且在一个共同犯罪中,因此属于包括的一罪,亦仅以一罪论处^[7]。

其二,为了在提高信息整合效率的同时尽可能地降低信息泄露风险,当前各类支持共享文档的应用程序均配备了强大的安全管控功能,以实现多层级的权限设置与精细化的行为管控。一方面,相关程序可以以主体为标准,为不同主体分配只读、编辑、分享等不同权限,例如石墨文档中的“千人千面”权限体系;另一方面,可以以文档内容为标准,为不同部分的内容设置具有查看、编辑等权限的人员范围,甚至可以具体到每一个独立的单元格,实现对信息界限的精准管控。不同的权限配置会对各主体行为的认定产生不同的影响,因此在探讨行为规制问题时应当将这一因素考虑在内。具体而言:(1)若创建者在创建共享文档之初即设置访问、编辑等权限范围,则其对于转发者将文档内容转发给权限范围之外主体的行为不承担责任,这里的转发行为主要采取拍照、摘抄、制作副本等形式,由于不具备相应权限,其他人无法访问或编辑直接转发的共享文档。(2)若权限范围外的主体获取共享文档中的个人信息,则属于非法获取,且其行为对象为非公开信息,因为文档中的内容仅针对有限者公开,属于限定范围的公开信息,由此其非法获取行为不具备合理处理这一违法阻却事由。(3)由于权限的设置,除前述主体外,还可能存在仅能够访问、读取文档内容但无法进行任何其他操作的主体,其行为方式主要表现为持有,对此可参照前述关于持有行为的规制路径。(4)创建者应当设置权限而未设置时,例如某公司人事专员在利用共享文档收集员工身份信息后未按要求设置访问权限,导致该文档中的个人信息被泄露,则需要根据其主观心态对其责任予以认定,若其具有故意,可能构成侵犯公民个人信息罪,若其仅有过失,则不构成本罪,但

非法获取相关信息的无权限主体仍有可能成立犯罪。(5)部分共享文档设置有访问密码,密码是获取操作权限的唯一凭证,若行为人泄露密码,虽然其未直接将文档中的个人信息转发给他人,但由于其行为使他人得以获取处理相关信息的能力,因此亦属于非法提供,且行为对象为非公开信息,对于获取密码者则需要根据其具体行为方式来判断其法律责任。(6)权限的设置共享文档信息整合过程中,对于确定责任主体也具有程序上的积极作用,即提供相应的证据支撑,例如根据权限设定,某部分单元格只能由某些主体访问与编辑,若此部分单元格中的个人信息泄露,则能够直接锁定责任主体的范围。

三、共享文档信息整合中公民个人信息的数量认定

侵犯公民个人信息罪以“情节严重”为入罪门槛,根据《解释》第5条的规定以及司法实践的具体情况,“信息类型与数量”是最为典型、适用最频繁的认定标准^[18]。《解释》第5条采取分级分类保护体系,对于高度敏感信息、一般敏感信息、普通个人信息分别设定50条、500条、5000条的界限,一旦相应类型的涉案信息超过该界限即属于“情节严重”,超过十倍以上即为“情节特别严重”。可见在侵犯公民个人信息类犯罪中,信息数量的认定对于罪与非罪的判断与刑罚轻重的裁量至关重要^[19]。如前所述,在共享文档信息整合的场合,各类主体的行为在特定情形下可能符合侵犯公民个人信息罪的行为要件,但罪名最终是否成立还需要结合涉案信息数量进行综合判断,而共享文档本身所具有的特性导致其中信息数量的认定并非完全与传统本地文档一致,因此需要进行特殊考量。

(一)基本认定规则

在共享文档信息整合场景下,文档内会形成一个“信息池”,所有填写者输入的信息均会呈现在文档之中。但“信息池”内的信息数量属于涉案信息总数,对各主体的定罪量刑应以其具体行为所侵犯的信息数量为准。前文已分别对各类主体相关行

为的刑法规制进路进行了具体探究,其中创建行为、修改行为不构成侵犯公民个人信息罪,因此在数量认定时不再对其加以考量,而仅关注转发、填写、副本制作、持有等可能构成犯罪的行为类型。

转发行为中的信息数量认定。其一,若转发时文档中已有信息,则属于侵犯公民个人信息罪中的“提供”,信息数量按已有信息认定,转发后其他主体填写并显示于文档中的信息不包含在内,毕竟对于此部分信息而言,转发者仅提供获取之平台,而非信息本身。其二,若文档中无信息,即仅对他人获取或提供信息予以帮助,信息数量按实行行为所涉信息认定。对于创建者而言,其创建共享文档之初即具有通过该文档整合信息的目的,且其明知共享文档的相关特性,因此其对后续其他主体的各类行为均应有预见性,尤其是在未设任何权限范围的情况下,若其仍然实施转发行为,则应对文档创建后其他所有主体的全部行为承担责任,所涉信息数量应为文档之中的全部信息总数。对于转发者而言,其仅对自身转发所造成的他人之获取、提供行为承担责任,而与之无关的部分,即使属于同一共享文档,亦不应被包含在内。例如,创建者将共享文档转发给A、B、C三人,A又将该文档转发给D、E、F,A仅需对后三者的行为负责,在数量认定时应将D、E、F行为所涉信息与A自身行为所涉信息合并,但B、C行为所涉信息则不应被包含在内。其三,若转发者明确要求接收者填写信息,则属于侵犯公民个人信息罪中的“获取”,信息数量按实际填写数量认定。

填写行为中的信息数量认定。一般而言,填写者所提供的信息数量应按其输入文档中的信息予以认定,但由于任何文档接触者均能获取文档中所载信息,因此填写者实则面向所有文档接触者实施提供行为,此时填写行为所涉信息数量应如何认定?向不同主体提供个人信息的行为使得信息的传播范围更广,各行为之间形成一种并联关系,因此《解释》第11条第2款在考虑传播面以及社会危害性的基础上规定应对涉案信息数量进行累计认定。但需要注意的是,面向不同主体实施的提供行为所针对的信息具有同一性,所侵害的法益也具有同一性,在行为人第一次向他人非法出售或提供该信息

时,已经侵害信息主体对相关信息所享有的信息自决权,后续的行为只是对这一法益的再次侵犯,为了避免重复评价,后续行为与之前行为所涉个人信息相同的部分不应再被累计认定。另外,在共享文档无任何权限设置的情况下,其中所载个人信息面向所有主体开放,此时个人信息接收主体并不确定,无法进行累计认定。当然,向多个主体出售或提供同一公民个人信息行为的传播范围必然大于仅向单一主体出售或提供,但其所造成的这种更为严重的影响通过在同一法定刑幅度内选择更重的刑罚加以量刑即可。

副本制作行为中的信息数量认定。虽然副本制作行为本身并不属于“获取”,但若行为人将副本泄露,则与传播本地文档无异,构成侵犯公民个人信息罪之“提供”,信息数量应当按副本所承载的数量认定。副本制作人必然可以接触共享文档并获知其中所记载的个人信息,在其获取行为本身非法的情况下,根据《解释》第11条第1款的规定,非法获取行为与传播副本行为所涉信息数量不能重复认定。因为二者所侵害的对象与法益具有一致性,在行为人实施非法获取行为时就已经侵害了信息主体对于涉案信息的信息自决权,待到其实施接下来的非法提供行为时,所侵害的仍然是相同主体对于相同信息所享有的权利,而这一法益在先前行为中已遭受损害,因此不再重复认定后行为中的信息数量。

持有行为中的信息数量认定。对于持有行为,若行为人持有共享文档后,其中所承载的信息由于他人的填写而持续增加,行为人获取的信息数量除包括持有文档时其中已有的信息,还应根据其主观故意的范围延展至后续所增加的信息,只要行为人明知其后他人仍会继续填写且具有获取故意,则此部分信息就应被包含在内,若无获取故意,则阻却犯罪成立。但后续增加信息的数量认定并非没有任何限制,某一行为人所涉信息具体数量截止于该行为人被抓获之时,其后输入的信息则不应被包含在内,至于如何确定其被抓获时信息数量增加的节点,则取决于司法机关获取并固定下来的相关证据。

(二)特殊情形处理

上述信息数量认定标准仅针对共享文档信息整合的最基本行为样态,由于共享文档所具有的多人协同编辑、内容实时更新等特性,在基本行为形态之外往往还存在众多特殊情形,对于后者中信息数量的认定需要予以特别关注,而这也是共享文档与传统本地文档信息整合的重大区别之一。

共享文档内信息内容的实时更新并非仅体现为数量的持续增加,还包括修改、删除等。如果行为人实施完毕符合侵犯公民个人信息罪行为要件的“获取”“提供”行为之后,共享文档中的信息内容发生变化,则应当如何认定涉案信息数量?例如在行为人所持有的共享文档中,他人填写个人信息6000余条,但由于期间其他主体的删除、修改等操作,待到行为人被抓获时,文档内信息仅剩4000余条,此时应按哪一时间节点的文档内信息对涉案信息数量进行认定?本文认为,他人将其所掌握的个人信填写入共享文档后,持有行为人由于持有该文档并可访问文档内容,因此立即取得处理相关信息的能力,应当认定为已获取这些信息^[20],即使之后其他主体删除、修改之前已存在于文档中的信息,也属于行为人既遂后出现的情形,不影响行为性质及信息数量的认定,因此涉案信息数量应以文档内信息最多时为准。需要注意的是,在行为人被抓获时,文档内信息已经发生改变,要确认文档内信息最多时的数量,需要对文档内容进行回溯,而当前市面上已有的共享文档应用程序均支持编辑历史和操作日志追溯,相关主体获取权限后即可访问该文档的所有历史版本,因此在技术层面保障了回溯的可能性。

为有效降低文档内容的泄露风险,部分创建者在初始创建共享文档时,除相关权限外,还设置了文档的有效期。无论是原始文档,还是转发链接,在有效期届满后均不得访问、编辑。这里的有效期与相关权限一样,均可指向特定主体,因此部分主体因时间届满而无权操作并不会影响其他主体权限的存续。有效期届满的主体所涉信息数量应以截止日期为时间节点,仅认定截止日期之前文档中已经存在的个人信息,此时仍需要结合行为人主观心态予以综合判断,之后继续增加但该主体已无法

获知的信息不应被包含在内。由于创建者修改权限设置,导致部分主体自某一时间节点开始无法访问、编辑共享文档,此情形中涉案信息的数量认定与前述场景相同。

在共享文档信息整合中,涉案信息数量通常较大,若要司法工作人员逐一核对,则将耗费大量人力、物力、财力,不仅效率低,还会造成司法资源的极大浪费^[21]。《解释》关于批量认定的规则有效地解决了这一问题,根据第11条第3款的规定,司法工作人员直接依据查获的信息数量进行认定即可。而在共享文档信息整合中,相关文档均内置有智能统计工具,能够更加高效地统计出文档内的信息数量,便于批量认定的进行。在得出涉案信息数量的初步结论后,还需排除其中虚假或重复的部分^[22],此处的虚假信息是指信息内容本身虚假,例如17位的身份证号码,至于该信息是否符合共享文档的主题则在所不问。

四、结语

共享文档在变革传统信息整合的行为样态、大幅提升信息整合效率的同时,也不可避免地产生了相应的刑事风险,这些风险对公民个人信息权益及与之关联的人身、财产安全造成严重威胁。本文基于类型化思维,结合共享文档信息整合过程中参与主体的多样性,主张应分别对不同主体之典型行为类型的刑法规制进行分析与研究,判断相关行为是否符合侵犯公民个人信息罪之行为要件,进而探寻刑法应对前述风险的具体路径。涉案信息数量的认定对于行为人罪与非罪的判断与刑罚轻重的裁量至关重要,因此不仅应关注共享文档信息整合中信息数量认定的基本规则,还应考量由于多人协同编辑、内容实时更新等特性所导致的特殊情形的处理。本文将研究视角聚焦于共享文档信息整合这一特殊场景内所存在的刑事风险及其刑法应对,但作为“云时代”新近出现的智能工具,共享文档的使用对现有法律制度的冲击远不止于此,其所带来的其他领域内的法律风险问题有待于后续相关研究予以明确。

注:

① 此处所谓信息整合,指的是将个别的、碎片化的个人信息汇集起来,从而形成一个有机整体,实质而言,其并非某一单独行为,而是涵盖个人信息从分散到集中的全部环节,包括信息的收集、获取、提供、转发、修改等。

参考文献:

- [1] 汤建华.健康医疗大数据共享风险及法治因应[J].学习与实践,2023,(8):54-60.
- [2] 蒋敏娟.跨域政府数据共享:实践探索与未来展望——以长三角地区为例[J].人民论坛·学术前沿,2023,(14):102-111.
- [3] 刘宪权.人工智能时代的刑事风险与刑法应对[J].法商研究,2018,(1):3-11.
- [4] 马改然.新技术对刑法个人信息保护的挑战与破解路径[J].中国政法大学学报,2023,(3):245-261.
- [5] 刘仁文.论非法使用公民个人信息行为的入罪[J].法学论坛,2019,(6):118-126.
- [6] 张昊.依法从严惩治侵犯公民个人信息犯罪[N].法治日报,2022-12-08(003).
- [7] 银昕.“华住开房记录泄露案”该如何处罚[J].中国经济周刊,2018,(45):42-43.
- [8] 储陈城.刑法应对网络暴力的流变及其基本立场[J].中国刑事法杂志,2023,(4):35-52.
- [9] 周光权.侵犯公民个人信息罪的行为对象[J].清华法学,2021,(3):25-40.
- [10] 刘双阳.“合理处理”与侵犯公民个人信息罪的出罪机制[J].华东政法大学学报,2021,(6):57-72.
- [11] 黄陈辰.论公开信息的刑法保护[J].大连理工大学学报(社会科学版),2022,(3):84-91.
- [12] 高铭暄,马克昌.刑法学[M].北京:北京大学出版社,2022.193.
- [13] 彭训文.助力防疫,平台有新招[N].人民日报海外版,2022-04-22(008).
- [14] 姜涛,郭欣怡.已公开个人信息刑法规制的边界[J].学术界,2023,(3):95-111.
- [15] 刘宪权,宋子莹.非法使用个人信息行为刑法规制论[J].青少年犯罪问题,2022,(4):64-73.
- [16] 张东生,戴有举.侵犯公民个人信息罪问题研究[J].河南财经政法大学学报,2018,(3):64-71.
- [17] 张明楷.刑法学[M].北京:法律出版社,2021.481.
- [18] 李静然,王肃之.侵犯公民个人信息罪的情节要素与数量标准研究[J].法律适用,2019,(9):69-76.

- [19] 简洁.公民个人信息类型和数量如何认定[N].检察日报,2021-10-12(007).
[20] 黄陈辰.侵犯公民个人信息罪行为要件的教义学重释——从“主体间移转”到“利用能力新增”[J].北方法学,2023,(5):106-115.
[21] 喻海松.侵犯公民个人信息罪司法疑难之案解[J].人民司法,2018,(32):13-16.
[22] 蔡云.公民个人信息的司法内涵[J].人民司法,2020,(2):24-26.

【责任编辑:周濛】

Criminal Risks and Criminal Law Response in the Process of Information Integration through Shared Documents

HUANG Chen-chen

(Law School, Minzu University of China, Beijing, 100081)

Abstract: Compared to traditional local documents, shared documents with real-time collaboration as the main feature are more conducive to improving information integration efficiency and ensuring real-time updates of information content. However, they also provide a breeding ground for crimes that infringe on citizens' personal information, leading to upgraded criminal methods, new crime scenes, a larger amount of involved information, and a wider range of information circulation. This type of criminal risk poses a serious threat to citizens' personal information rights and their associated personal and property rights, and urgently requires criminal law to address it. The process of using shared documents for information integration involves multiple subjects such as document creators, retweeters, fillers, modifiers, replica creators, and holders. Each subject assumes different roles and has differences in specific behavior. Based on typological thinking, typical behavior types of different subjects should be considered separately to determine whether they meet the behavioral requirements of the crime of infringing on citizens' personal information, and to determine the specific path of criminal law regulation. The amount of information involved in the case is crucial for determining whether the perpetrator is guilty or not, as well as for determining the severity of the punishment. When determining the quantity, attention should not only be paid to general identification rules but also to the handling of special situations caused by the collaborative editing and real-time updating of content by multiple people in shared documents.

Key words: shared documents; criminal risks; the crime of infringing on citizens' personal information; public information; quantity determination