武漢大學學報(哲学社会科学版)
WUHAN UNIVERSITY JOURNAL (Philosophy & Social Science)
第75卷第1期 2022年1月
Vol. 75 No. 1 Jan. 2022 143~156
DOI:10.14086/j.cnki.wujss.2022.01.013

《个人信息保护法》中"知情同意条款"的出罪功能

李立丰

摘 要 《个人信息保护法》明确的知情同意原则是事先预防型个人信息保护机制的重要体现。在对知情同意原则加以合理完善的基础上,可将以"移动应用程序"(APP)隐私政策为代表的告知同意条款,视为个人信息处理者与个人信息主体之间达成的合意,而这种合意与刑法中作为出罪事由的"被害人同意"之间存在实质契合关系。在刑事合规的语境下,个人信息处理者应对隐私政策文本作出调整,以保障用户的知情权。针对可能给个人信息背后的多重法益带来风险的处理行为,个人信息处理者必须告知用户相关行为及伴随的风险并征求用户同意,借此完成从单纯的个人信息保护原则向个人信息保护与利用之平衡原则的转变,同时帮助个人信息处理者规避侵犯公民个人信息等刑事责任。

关键词 《个人信息保护法》;隐私政策;知情同意原则;出罪事由;网络平台刑事合规;信息网络犯罪;个人信息自决权;移动应用程序

中图分类号 D914 **文献标识码** A **文章编号** 1672-7320(2022)01-0143-14

基金项目 吉林大学横向课题(TY2019-FW129-ZFCG129);吉林大学哲学社会科学青年学术骨干支持计划(2016FRGG05)

2021年11月生效的《中华人民共和国个人信息保护法》(下文简称《个人信息保护法》)继承并进一步明确了知情同意原则。反观我国学界,对于知情同意原则所保护对象的范围,仍存在巨大争论。例如,个人信息主体享有的是"权利"还是"利益"[1](P146);个人信息是否属于私法的保护对象[2](P35);个人信息权与隐私权是否存在区分之必要[3](P118)。其中,关于个人信息权利是否存在的论争,虽在民法学界意义重大,但在刑法学中不存在深究的必要,因为法益概念可被视为"权利"和"利益"的统称,这与一些民法学者所主张的"个人信息权益"概念包括"本权权益"与保护"本权权益"的权利的观点不谋而合[4](P1147)。然而,个人信息究竟属于公共物品还是应由私权来保护这一问题,直接决定了侵犯公民个人信息罪的体系定位是否合理,这对刑法学研究来说颇具意义。个人信息权与隐私权之区分是否必要的问题,也会影响到侵犯公民个人信息罪的法益确定,进而左右相关出罪事由的讨论。故有必要在行文之前,对这两个前置性问题加以回应。

首先,个人信息并非公共物品。虽然信息主体对其个人信息所拥有的权利,不具有物权的独占性(典型例证如,为了国家利益之需要可以收集个人信息),而且一旦将个人信息提供给个人信息处理者使用,信息主体就丧失了对其个人信息的实际控制与支配,但是,对于信息主体而言,个人信息具有人格自由与人格尊严价值,承载着多重法益(包括隐私、人身、财产利益),仍然属于民法中私权的客体。在这个意义上,侵犯公民个人信息罪被规定在《中华人民共和国刑法》(下文简称《刑法》)第4章"侵犯公民人身权利、民主权利罪"中,是合理的。

其次,《个人信息保护法》第4条规定:个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息。其中既包括自然人不愿为他人所知的私密信息,也包括姓名、电话号码、政

治面貌等在社会交往中必须向他人提供以确立自身人格外观的一般个人信息,所以个人信息(权益)与隐私(权)之间存在区别。刑法中侵犯公民个人信息罪中的犯罪对象是公民个人信息,根据法秩序统一原理,本罪的法益应当至少包括个人信息权益。认为本罪保护的是隐私权的观点,显然不当缩小了本罪的保护范围。

在回答了上述前置性问题之后,便可正式提出本文旨在解决的问题,即在个人信息处理者与用户的互动关系中,知情同意原则是否被视为侵犯公民个人信息罪的出罪事由。首先,本文以"移动应用程序"(下文简称"APP")为例,研究作为个人信息处理者与用户互动规范的隐私政策的属性。其次,针对知情同意原则所面临的现实困境提出应对方案。再次,结合改善前后的知情同意原则,探讨其与刑法语境下"被害人同意"的关系。第四,讨论将完善后的知情同意原则作为侵犯公民个人信息罪出罪事由的可行进路。最后,明确知情同意原则出罪功能的适用限制,以实现企业刑事合规与个体权益保障之间的平衡。

一、APP隐私政策的合同属性

作为"典型"的个人信息处理者,APP的经营主体在其与用户的互动关系中,主要通过隐私政策的文本设计与适用来落实知情同意原则。因此,对于APP隐私政策属性的认定,直接影响到知情同意原则与侵犯公民个人信息罪的关系。

(一)我国APP隐私政策的现实样态与属性论争

我国主流APP的隐私政策文本,基本上都倾向于将隐私政策视为用户与APP经营主体之间的合同。如《支付宝隐私政策》提示用户需要同意其按照该政策约定处理用户的信息。《淘宝平台服务协议》同样明确淘宝平台的隐私权政策是该协议的补充协议,与其不可分割且具有同等法律效力。据此,一般认为我国APP的隐私政策,是指用户与APP运营者之间的协议或约定,即合同。然而,现实样态却并非如此简单。以安卓系统客户端多款APP为例,其隐私政策大体分为两类:第一大类,如百度、抖音、淘宝、知乎等,用户下载安装后首次点开该APP时,隐私政策的链接就会出现。而其可以进一步细分为"要么同意,要么离开"类以及"注册需同意"类。属于前者的APP用户,如果不同意相关隐私政策,就根本不能使用该APP的任何服务。属于后者的APP用户,即便点击"不同意"也不会退出,仍能使用相关APP的部分服务(如知乎里游客模式下的浏览服务),但是如果想要使用相关APP的核心服务,就必须同意隐私政策,注册或登录后才能使用。在这种情况下,如果承认APP隐私政策属于合同,那么合同的双方显然是APP与注册用户,而不是仅仅使用浏览服务的"游客"。这就意味着,如果承认APP隐私政策的性质属于合同,那么点击"同意"的用户与这一大类APP之间就会由此产生契约关系。第二大类,如拼多多,用户在下载安装完毕首次点开该APP之时,并不能直接看见隐私政策,在个人中心—设置中也不能看见隐私政策,而是需要注册登录之后,才能在APP的个人中心—设置中找到该APP的隐私政策。这就会导致一个看似矛盾的问题,即用户同意该类APP隐私政策的时间,甚至早于用户发现或浏览隐私政策内容的时间。拼多多APP隐私政策明确表示,一旦用户开始使用拼多多的各项产品或服务,即表示已充分理解并同意本政策。这就意味着用户只要安装该APP之后进入相关页面简单浏览,即等同于用户表示同意。然而,用户这个时候尚未注册,对于后面才能阅读到的APP隐私政策内容一无所知。如此一来,如果认为此类APP隐私政策具有合同属性,那么该合同的成立生效时间显然早于合同一方当事人得知合同内容的时间。

对此,我国学界存在两种观点。有学者认为经用户同意的隐私政策将在用户与网络服务提供者之间成立合同关系,其与网络服务协议是相互独立的两个合同,是网络服务协议的前置性协议,而不需要经用户同意的隐私政策属于企业自律规则。但从实践来看,在许多情形下,隐私政策需要经过用户同意才生效[5](P129-133);有学者认为,经营性互联网信息服务网页上所载的隐私政策是网络经营主体与网

络用户就收集、存储和使用用户个人信息的行为进行的约定，为格式条款合同。非经营性网站上所载的属于告示类的隐私声明不是合同[6](P209)；还有学者从网络免费服务的本质出发，认为用户如果不授权企业对个人信息的使用则无法享受网络经营者的服务，个人信息的授权与企业的服务形成对价关系，企业发布隐私政策是要约，用户选择企业的服务，则表现为用户对隐私政策的同意。此外，隐私政策合同说还可以通过隐私政策的内容进一步证明[7](P133)。然而，有学者认为隐私政策根本不是合同，不具有合同属性，而是“具有社会承诺属性”[8](P27)，主要理由是消费者个人信息蕴含着社会价值，因而隐私政策必须符合公共利益；强调个人信息的社会控制意味着个人信息的使用应由社会决定，而非由个人决定；不管用户是否真正同意隐私政策，监管机构、媒体等都可以对企业的隐私政策反复评价，企业的隐私政策因而代表了企业的社会形象；协议所应有的协商和合意在提供与接受隐私政策的过程中荡然无存，用户要么同意，要么离开。所以，隐私条款因具有社会属性而不再是APP经营主体与用户之间的合同。

（二）APP隐私政策的民事合同性质

本文认为，APP隐私政策属于个人信息处理者与个人信息主体之间缔结的民事合同。首先，不能以个人信息的社会控制论为依据否认隐私政策的合同属性。个人信息社会控制论否定信息主体对于个人信息绝对的、普遍的控制，提倡建立“以一般允许为原则，以个人控制（同意决定）为例外”的个人信息使用规则[9](P99)。也就是说，这种观点其实并不否认存在应当由用户个人控制或支配的个人信息。其次，隐私政策中依旧存在用户与APP之间的协商与合意，“不同意，就退出”的现象实际上是不存在的。从形式上看，某些APP的用户的确只有选择同意全部隐私政策，才能进入相关页面，否则将被迫退出。但事实上，即便用户选择接受，仍然可以通过在设置中行使默认不开启的权限等方式，对APP隐私政策中的某些条款做出后续调整。也即，对于隐私政策中涉及个人信息采集的关键条款，用户仍然可以自主选择同意或不同意。例如支付宝的隐私政策虽然建议用户为了更安全、便捷地登录，可选择刷脸登录服务，并向支付宝方面提供脸部图像或视频，以核验用户身份。但用户如果选择不同意，并不会被强制退出。在这个意义上，“要么同意，要么离开”的情况并不全然或绝对存在。毕竟几乎所有APP隐私政策条款都规定，如用户不同意提供前述信息，将无法完成（上述）特定操作，但不影响使用其他服务等内容，例如，淘宝用户如果拒绝提供上述信息，虽然无法注册淘宝平台账户，但仍可以使用浏览、搜索服务。换言之，存在某种用户选择空间。因此，本文认为隐私政策就是个人信息处理者与个人信息主体在互动关系中形成的以个人信息处理与保护为主要内容的合同。

判断APP隐私政策属性的意义在于：隐私政策的属性决定了用户的知情同意是否可以成为侵犯公民个人信息罪的出罪事由。如果APP隐私政策构成个人信息处理者与个人信息主体之间的合同，那么尽管APP隐私政策可能存在违背现行管理性法律规范的条款，但是对于这些条款用户仍可以同意，即经同意的此类条款仍属于有效的合同条款。而所谓管理性强制规定是指，法律没有规定违反该强制性规定将导致合同无效，违反该规定亦不损害国家利益和社会公共利益，只是损害当事人利益[10](P341)。违反管理性规定承担的是被管理一方的管理责任或行政处罚。由此可见，《中华人民共和国民法典》（下文简称《民法典》）第1035条或《个人信息保护法》第5条规定的个人信息处理的必要原则属于管理性规定。我国现行法律、行政法规等禁止APP过度收集用户个人信息，但是在APP隐私政策是合同的前提下，在隐私政策中约定的过度收集个人信息的条款虽然违反强制性管理性规定，但经过用户同意，过度收集条款仍然有效，即用户对违反强制性管理性规定的条款之同意有效。所以按照隐私政策（合同）中过度收集条款实施的过度收集行为，虽然“违反国家有关规定”，侵犯了公民个人信息不被过度收集的个人信息权，因而该当侵犯公民个人信息罪的构成要件，但是可以在违法性判断意义上研究用户知情同意是否阻却违法性。然而，如果隐私政策是APP经营主体的自律规则，鉴于企业自律标准不应该低于现行国家有关规定中个人信息保护标准以及国家标准，所以在隐私政策中不能规定有违反国家有关规定收集或提供个人信息的条款。而且，因为自律规则不需要经过用户同意，故不可能存在用户同意是否阻却“违反

国家有关规定”的收集或提供行为违法性的问题。如果隐私政策是自律规则,那么本文所研究的知情同意与侵犯公民个人信息罪的关系则毫无意义。正因如此,本文于正文之首,直截了当提出隐私政策属性之疑问。

二、知情同意原则功能失灵的应对

通说认为,知情同意原则是指信息经营主体在收集个人信息之时,应当对信息主体就有关个人信息被收集、处理和利用的情况进行充分告知,并征得信息主体明确同意的原则[11](P76)。知情同意权是个人信息权的积极权能之一,可分为知情权和同意权。知情权是指数据主体有权知道与其数据将被处理的一切相关资讯,包括数据控制人的身份、拟处理数据的范围、处理依据,等等。在这个意义上,知情是同意的前提,同意是知情的目的,同意的对象是一切形式的数据处理[1](P152)。还有论者认为,告知是同意的内在规范要求[12](P125)。但在另一方面,知情同意原则在适用过程中面临挑战,存在功能失灵的可能。

(一)针对知情同意原则功能失灵的应对策略

知情同意原则面临着两大挑战:第一,不告知影响用户选择的决定性信息,使得同意丧失了有效性基础。APP 隐私政策作为保障用户知情同意的主要方式,往往只告知用户 APP 收集的个人信息的范围等内容,以及不提供个人信息就难以享受某些服务的后果,却并没有提示用户相应处理行为可能引发的风险。事实上,个人信息类型繁多,其附着有用户的人身利益、财产利益、隐私利益,处理行为可能会给这些利益带来风险。例如:收集私密信息并对其做进一步的处理,可能对私密信息所承载的用户隐私利益造成风险;或者,以作为处理方式的存储为例,因为存储技术自身的原因,个人信息极有可能在存储期间被窃取或泄露,但是因为未告知相应风险,普通用户根本无法预测该处理行为可能引发的风险及其程度。而根据目前我国法律之规定,用户需要自行对处理行为的风险加以判断或预测,然后做出是否同意的决定。在缺乏对行为风险预见能力的基础上的同意,难以被视为具有法律意义。第二,知情同意原则的实现成本过高。对于用户而言,阅读动辄上万字的隐私政策需要花费大量时间,容易造成用户阅读困难。文本长度过短,势必不能全面展示隐私政策内容[13](P76),导致有些处理行为其实没有征得用户同意。对于 APP 经营主体而言,终究是以营利为目的,适用知情同意原则可能与其作为营利性实体的本质存在龃龉。

面对上述挑战,持“彻底抛弃说”的学者认为在大数据时代,应及时转变思路,转变知情同意的固化思维,借鉴秉持个案分析精神的欧美场景与风险导向理念,将“在具体场景中合理”作为个人对个人信息处理行为的合法授权[3](P109)。但这种观点存在如下难以回避的问题:首先,个人信息的知情同意原则不仅仅适用于个人私密信息,也适用于个人一般信息,而处理一般个人信息的行为未必会带来隐私风险。法律规定知情同意原则除了具有要保护个人隐私的意图之外,更重要的是想借此保护个人信息自决权,保障个人信息的人格自由与人格尊严价值。因此,仅以隐私风险为判断处理行为合法性的标准,是对个人信息自决权的忽视,故与《民法典》以及《个人信息保护法》的立法趋势相悖。其次,具体案件中的隐私风险是否能为该案中的信息主体所接受,并没有明确的判断依据。本文认为,在大数据时代,各种计算机技术及其对个人信息处理的具体方式、风险、结果难以被不具有计算机专业知识的普通用户所知,根本无法得知用户预期的风险是什么,甚至用户自己都不知道自己是否预期过处理行为的风险。与此相对,持“完善说”的论者主张,应以《民法典》第 109 条规定的人格权保护的价值基础为界分基准,对个人信息处理行为加以分类,触及人格尊严和自由发展的个人信息处理行为适用明示同意,而与人格尊严和自由发展无涉的个人信息处理行为适用默示同意(从用户使用 APP 的行为可以推断出用户的默示同意)[14](P100-101)。但是本文认为这种分类标准过于抽象,在实践中难以判断何种处理方式关涉人格尊严与自由发展,因而其完善方法不具可操作性。除此之外,有论者提出“弱同意模式”,主张用户的沉默

（拟制同意）代表同意个人信息处理行为，而拟制同意适用的前提是情境合理标准[15]（P81-82）。这种观点其实是借鉴了欧美的场景理论与风险理论，主张情境是场景与规则的统一，但是何谓场景、其构成因素有哪些以及规则有哪些，则根本没有明确，所以该规则不仅不能起到完善作用，还可能带来新的麻烦。此外，对于有论者所主张的通过加强隐私政策界面友好度以及坚持最小收集原则来完善告知同意原则的观点，存在如下问题：第一，鉴于用户与APP经营主体的谈判筹码相差悬殊、用户对大量的隐私政策感到麻木、对遥远的潜在风险不敏感等因素，只是在形式上加强隐私政策文本界面友好度，对于“同意”难以起到实质帮助。第二，目的限制原则的功效很容易被笼统的目的如“为了改善您的服务体验”等削弱。第三，核心功能与非核心功能的界分目前没有统一标准，并且APP经营主体很容易通过降低用户体验度的方式迫使用户追加授权，所以以此为基础的区分授权难以实现。第四，在数据聚合技术的加持之下，即使APP只收集了用户的非敏感信息，但是一经与该用户的其他零散一般个人信息甚至APP从其他用户处收集的个人信息相结合，APP经营主体很有可能已获知该用户的敏感个人信息，从而使得个人一般信息与个人敏感信息的区分几乎丧失了必要性。

（二）应双管齐下完善知情同意原则

本文认为，我国《民法典》以及《个人信息保护法》将知情同意原则作为保护个人信息权的主要手段，而同意原则又是事先预防型个人信息保护机制的重要体现，废除同意原则的后果，必然是整个社会将注意力转向侵犯个人信息的事后救济，最终导致某些权益无法得到充分保障。因此，在大数据时代，知情同意原则仍具有存在意义，同时也应予以完善。

完善知情同意原则必须注重APP经营主体与普通用户之间的利益平衡，而不能一味赋予个人信息自决权以绝对保护。毋庸讳言，用户才是个人信息的来源以及原始权利人，但是个人信息不仅仅对个人有人格自由与人格尊严价值，个人信息还具有商业价值和社会管理价值[16]（P10）。因而不能片面地从保护人格自由与人格尊严的视角，而要站在兼顾个人信息对个人的人格利益以及个人信息对个人信息处理者的经济利益的角度，审视知情同意原则。同时，为了实现用户的人格利益与个人信息处理者对个人信息的利用之平衡，应采取两条路径完善知情同意原则。其一，合理处理行为不需经过用户的同意，以对同意权加以限制。其二，隐私政策中应告知可能给个人信息背后的用户隐私利益、财产利益、人身利益带来潜在风险的处理行为的风险程度，以便完善其行使个人信息自决权的基础。借助路径一，个人信息对企业的商业价值或对社会公共利益的价值可以得到最大发挥。借助路径二，可以使个人对个人信息处理行为的自决权，或者说用户个人信息自决权以及其对个人信息上多重法益的自决权落到实处。因此，路径一与路径二双管齐下，可以在平衡个人信息处理者的利益与用户个人信息自决权的前提下，实现对知情同意原则的完善。

本文认为，不会给个人信息背后的用户隐私利益、财产利益、人身利益带来任何风险且有利于增加企业经济利益或社会公共利益的处理行为，都是合理处理行为。我国法律规定，个人信息处理者收集使用个人信息时应告知信息主体并且获得其同意，从信息主体权利角度来看，这是为了保护其个人信息自决权，从更深层次而言，是为了保护个人的人格自由与人格尊严，而从社会治理的角度来看，是为了防止个人信息的不当运用妨害社会发展，如将用户个人信息用于实施电信诈骗等犯罪。而对合理处理行为的界定，不能以前者为依据或者将其作为依据之一，即不能认为只有经过了告知和同意，因而未侵犯人格利益的处理行为才是或才可能是合理处理行为。首先，个人信息自决权以及作为其基础的人格自由与人格尊严极其抽象，无法在被侵犯时让权利主体清晰感受到自己所承受的经济损失、身体痛苦或精神痛苦。因此，以未侵犯个人信息自决权及人格自由与人格尊严为标准界定合理处理行为，不具备可操作性，应当摒弃。本文对于合理性之界定不以人格自由与人格尊严为标准的观点，或许与个人敏感信息的界定不谋而合。《个人信息保护法》就是以泄露或滥用之后的后果为标准界定个人敏感信息。其次，个人信息处理者虽未告知用户，也未经用户同意，但纯粹为了合法的商业目的处理个人信息时，个人信息主

体一般不会遭受身体与精神痛苦,也不会遭受财产损失,甚至可能有利于提升用户的利益。此类行为既能够为企业改进产品或服务提供决策的数据支撑,也能够帮助个人信息处理者在APP中更精准地投放广告进而赚取作为其主要收入来源的广告费。在不威胁用户精神利益和财产利益的情况下,不仅有利于增加APP经营主体的经济利益,还有利于提高用户的服务体验,实现了用户与APP经营主体的利益平衡。因此,在确定合理处理行为的标准时,不威胁用户法益且能增进企业商业利益的情形理应被纳入考虑。最后,个人数据商业价值的充分发挥,能够促进数字经济以及移动互联网行业的发展,进而增加社会整体福祉。此外,对个人信息的创新性利用,极有可能为社会创造意想不到的价值。比如,谷歌(Google)公司最初并未将预测流感趋势作为数据分析的目标,而是偶然在合成各种大体量数据信息的基础上,得出了较为准确的对流感发病率及发病时间的预测结果[17](P67)。换言之,在考虑处理行为是否合理时,不威胁用户法益且增进社会整体福祉应作为考虑因素之一。综上,处理行为合理性的决定性因素有:未对个人信息上承载的隐私利益、人身利益、财产利益造成风险,且有利于增加企业商业利益之实现或有利于社会公共利益之实现。对于个人信息的合理处理行为,由于用户应当容忍或必然会同意,所以实际上该类处理行为不经过用户明示或默示授权也不会侵害到其同意权,问题在于是否需要将合理处理的行为告知用户?本文认为答案应该是:客观上能做到提前告知的处理行为,个人信息处理者应当单方告知用户,但是客观上做不到提前告知用户的处理行为无需告知。

本文还认为,风险识别以及预测的义务应由个人信息处理者承担。在隐私政策中告知个人信息处理行为的风险的前提条件是,作为个人信息处理者的APP经营主体明知其处理用户个人信息的行为会给用户的隐私、财产、人身法益带来何种程度的不利影响。我国司法实践中已经有判决开始意识到选择对用户同意的作用。例如,法院判定"用户是否自主选择,应在充分尊重用户及服务提供者双方意愿基础上,综合考虑用户的选择可能、选择能力、进行相应选择对用户的实质影响等因素予以判断"(北京互联网法院[2019]京0491民初16142号)。毋庸讳言,将风险识别以及预测的义务从用户转移到APP经营主体身上是妥当的。其原因在于,首先,与对大数据和计算机技术一无所知的普通用户相比,掌握大量数据以及数据处理技术的个人信息处理者显然能够更容易地了解处理行为的潜在风险。其次,为了预防因不遵循法律法规而遭受法律制裁的风险,个人信息处理者应当建立合规计划、完善合规管理体系,而有效合规计划的基本标准之一便是合规风险评估[18](P9)。而APP经营主体的合规风险评估的重要内容应当是,处理行为在何种程度上会给用户法益带来风险。虽然我国法律没有要求APP经营主体在隐私政策中需告知用户个人信息处理行为的潜在风险,但是我国2020年10月1日起实施的国家标准《信息安全技术个人信息安全规范》明确指出,个人信息保护政策中应描述用户提供个人信息后可能存在的安全风险。因此,规定由APP经营主体而非用户识别风险,更具合理性和可操作性。用户只有在清楚地了解处理行为对个人信息附着的多重法益的潜在风险程度之后,才能真正做出同意与否的决定。

三、刑法中被害人同意与知情同意原则的实质契合

如前所述,完善后的知情同意原则,为将隐私政策视为个人信息处理者与个人信息主体之间达成的合意,进而为探索该原则与刑法中被害人同意之间的关系奠定了基础,也为二者的实质契合创造了条件。

(一)被害人同意的出罪功能

大陆法系刑法采用阶层论,设置不法构成要件,旨在实现保护法益的目的。而这意味着,如果个人基于自我决定权,放弃了其有权处置的法益,刑法就没有必要为了保护法益而去违反法益主体的意思,国家刑罚权根本没有介入的必要[19](P247)。正因为这种自由意志决定的自主性,"得到承诺的行为不违法"成为公认的法谚。我国主流学说基于结果说的立场,将被害人同意和被害人自陷风险划分为两个不同的概念范畴。与此相对,一种较为有力的观点认为,被害人同意阻却违法性的理由在于危险行为符合

被害人的自我决定。也就是说，所谓“被害人”同意的是行为人实施危险行为，即使发生法益侵害结果，也不能将该结果归属于行为人[20](P57)。

尽管就目前而言，对于我国刑法中的被害人同意，还只能被视为一种超法规的出罪事由，但事实上，无论是相关司法解释还是具体的司法实践，都已经开始承认被害人同意的出罪功能。例如，根据2017年《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》（下文简称“两高解释”），未经被收集者同意，将合法收集的公民个人信息向他人提供的，属于《刑法》第253条之一规定的“提供公民个人信息”。这就意味着，只要得到了被收集者同意，就会阻却犯罪的成立[21](P162)。又例如，在“淘宝商铺信息转让案”中，被告人将得到公民个人同意、已开好了淘宝店铺的公民信息出售给他人的行为（广东省开平市人民法院[2018]粤0783刑初215号一审刑事判决书），以及行为人利用网络爬虫工具，从公开网站上获取企业及公民信息主体同意或授权公开的个人信息的行为，因为没有侵犯公民个人信息自决权，不应被认为构成相关犯罪[22](P31)。由此不难看出，即便就本文所讨论的主题而言，被害人同意的出罪功能都应当得到重视并展开进一步的深入探讨。

（二）被害人同意的成立条件

刑法中的被害人承诺（同意）的有效性条件包括，受保护的法益必须在原则上是可以处分的个人法益；承诺者必须有足够的洞察能力，即被害人必须有能力对法益侵犯的方式和程度以及相伴随的风险和后续的风险具体有所了解；承诺必须是事先同意，事后的批准是不够的；承诺必须以明示或默示方式表达出来；承诺不能是在被强制或被欺诈情况下做出的[23](P119-120)。有论者认为，被害人承诺正当化要件包括：对法益有处分权限；有承诺能力（对承诺的内容、意义、结果有理解能力）且承诺真实；承诺必须发生在行为发生时，最迟在结果发生前做出；法益侵害、危殆化行为必须在承诺范围内实施。承诺范围不仅仅包括侵害行为或具有危险性行为的性质、意义及此行为的范围，也必须囊括由该行为所产生的后果[24](P178)。还有论者认为，被害人承诺的有效条件包括：承诺者对被侵害的法益具有处分权限；具备承诺能力，即被害人对所承诺的事项的意思范围具有理解能力；不仅承诺行为，而且承诺结果；必须出于真实意愿；承诺不必表示于外，行为人也不必认识到承诺；承诺至迟必须存在于结果发生时；经承诺实施的行为不得超出承诺范围[25](P224-226)。

虽然关于被害人承诺的体系性地位存在争论，但是学者们对于其成立要件的观点大体是相同的。以上三位论者都是阶层论者，第一位认为被害人承诺是构成要件的阻却事由，后两位主张被害人承诺是违法阻却事由。而批判四要件犯罪构成体系的许多论者，认为被害人承诺位于四要件犯罪论体系之外，由此认为四要件犯罪构成体系应被抛弃[26](P113)。但是如果采取“被害人同意一元论”的立场，即个人自治的法益观，得到被害人同意的行为并没有侵害法益，当然也就没有侵害犯罪客体，所以四要件犯罪论体系之中仍然有被害人承诺之地位。知情同意原则之下的用户同意是否满足刑法上被害人同意的成立要件，关键在于用户是否对所承诺的侵害或危殆化法益的行为之结果有所了解。而满足完善之前知情同意原则的用户同意与满足完善之后知情同意原则的用户同意，在这一点上存在区别。

（三）知情同意原则的完善及其与刑法中被害人同意的实质契合

传统知情同意原则“要求自然人在个人信息被收集时就评估信息处理的潜在风险，同意时的成本（收益）考虑依赖于对未知风险的判断，因此存在结构性缺陷”[14](P90)。事实上，在个人信息被收集时，用户根本无法预测到信息处理行为（包括收集行为本身）对个人信息上所承载的隐私、财产、人身法益的风险。而被害人承诺要求被害人必须对“法益侵犯的方式和程度以及相伴随的风险和后续的风险具体有所了解”[23](P119)，也就是说，被害人不仅承诺行为，而且承诺结果。但是用户在其个人信息被收集时，显然无法得知处理行为（包括收集行为本身）的结果，因此可以认为用户对处理结果无法做出承诺。由此可见，完善之前的知情同意原则中的用户同意并不符合被害人同意的条件，进而无法成为APP经营主体即个人信息收集者的出罪事由。

大数据时代,数据聚合技术使得通过个人不敏感的信息可以分析出个人敏感信息,区块链技术使得个人信息在无限长的分享链条上流动,因而使个人信息暴露在被侵犯的巨大风险之下。由此可见,APP经营主体的个人信息处理行为给用户个人信息上承载的多重法益造成的风险委实难以为用户所预见。用户无法预测到行为人处理行为的风险,所以自然没有同意处理行为带来的风险,也可以说对处理的危害结果的所谓"同意"并无法律意义。所以,如果处理行为确实给用户法益带来风险,那么用户对隐私政策的同意,乃至针对特别告知,如APP经营主体通过弹窗展示的索取权限要求的同意,并不符合"被害人应了解行为附随风险"这一要求。

德国学者曾经指出,刑法中的被害人同意与民法中的意思表示制度十分相似,本质上与当事人在民事法律上通过民事法律行为创设权利和义务、招致特定法律后果的情形大体相同[27](P31)。进一步而言,无论是作为民法中的免责事由,还是刑法中的出罪事由,二者都建立在人的自我决定权基础之上,具有实质契合性。按照改进之后的知情同意原则,APP经营主体需要在隐私政策中明确告知用户,相关个人信息处理行为将会给其法益及个人信息背后的多重法益带来风险,以便用户在充分知情的情况下做出选择。符合改善后知情同意原则的用户同意,完全符合被害人同意所要求的洞察能力。因此,如果APP经营主体在隐私政策中告知用户处理行为及其风险,而用户对隐私政策表示同意,则用户的知情同意符合被害人同意的要求,威胁到个人信息背后的用户隐私、财产、人身法益的违反国家规定的处理行为便不构成犯罪。

四、侵犯公民个人信息罪中的被害人同意

《个人信息保护法》第71条规定:违反本法规定,构成违反治安管理行为的,依法给予治安管理处罚;构成犯罪的,依法追究刑事责任。在个人信息处理者的刑事合规语境下,本文选取侵犯公民个人信息罪作为样本,探讨将被害人同意作为个人信息处理者出罪事由的具体路径。

(一)知情同意的出罪功能

有论者认为,对于公民个人信息的刑法保护,建立在我国宪法对公民基本权利保护的基础上,侵犯公民个人信息罪的法益应是人格自由与人格尊严,隐私利益只是人格尊严保护的内容之一,该罪的法益是个人信息权中的个人信息自决权[22](P31)。有论者认为本罪法益是个人信息保密权,犯罪对象仅限于公民有保护要求且采取了保密措施的个人信息[28](P174)。有论者认为,本罪的法益是个人信息安全以及公民人身、财产、隐私以及正常的工作生活[29](P4)。还有论者站在本罪是抽象危险犯之立场,认为既然设置本罪的目的在于实现法益的前置性保护,那么本罪没有创设新的法益,本罪的法益仍是刑法中重点保护的人身、财产法益[30](P140)。这些论者的观点都认为侵犯公民个人信息罪只侵害个人法益。

持不同意见的论者在对侵犯公民个人信息罪的各种个人法益说展开批判之后认为,本罪之法益是个人信息安全的社会信赖,即社会成员对个人信息安全的信赖,立法者只是希望通过本罪来维持保障社会成员对个人信息安全的信赖,使社会成员安心参与社会活动,不因惧怕个人信息泄露而限缩自身自由活动范围[31](P148)。有论者认为,侵犯公民个人信息罪评价的根源不在于某个信息被单独违规使用,而在于行为的规模性(大规模不合理使用)和可预见的风险(导致严重后果),因而本罪的法益是社会信息管理秩序[32](P71)。还有论者综合了个人法益与超个人法益说,认为本罪是复杂客体犯罪,主要客体是名誉、隐私的人格权益,次要客体是国家和社会公共利益、秩序和安全[33](P116)。

本文认为,首先,从侵犯公民个人信息罪的体系地位来看,本罪的法益不能只是超个人法益。有学者以司法解释将侵犯个人信息数量多少作为情节是否严重,即是否构成本罪的决定性因素为由,认为本罪的法益是多数公民个人信息自决权的叠加,而信息自决权经叠加后难以被认为是个人法益。但实际上,罪量的要求固然算是我国刑事立法的特色之一,而体现这一特色的,并非本罪的法益,而是本罪的行为方式,即非法获取、出售、提供,对个人法益造成的侵害达不到直接用刑法制裁的程度,因此需要在罪

量上做出要求以使相关行为之社会危害性达到入刑的标准。其次，与其说本罪的次要客体是国家社会公共利益，不如说本罪的间接客体是国家社会公共利益。最后，不应将人格自由与人格尊严认定为本罪之法益，因为刑法上的法益概念应避免抽象化，人格自由与人格尊严作为一般人格权具有兜底保护功能，显然过于抽象。而将个人信息自决权或更准确而言的个人信息转移自决权作为本罪法益的论者，在分析本罪法益时，显然只关注了本罪实行行为本身，并没有考虑到设定该罪的立法初衷，且这种观点不当缩小本罪的评价范围。例如，某些未经同意的过度收集私密个人信息的行为，侵犯了个人信息自决权，同时也给个人信息所承载的隐私利益带来风险。如果认为本罪之法益只有个人信息自决权，显然无法评价本罪实行行为对隐私利益构成的风险，即这种观点缩小了本罪的评价范围或评价功能。

毋庸讳言，与转移自决权相比，使用自决权更值得受刑法保护，但是刑法迟迟没有增设使用型个人信息犯罪，除了既有犯罪可以规制非法使用（如将个人信息用于电信诈骗、敲诈勒索等）个人信息行为的原因之外，还可能是因为在涉个人信息犯罪的地下产业中，非法获取或提供是非法使用的上游行为，对上游犯罪加以打击与预防、对犯罪产业链的源头进行治理，可以更有效且及时地遏制下游犯罪之发生，等到非法滥用行为发生再进行打击显然为时过晚，于是只设立了对非法使用加以前置化打击的侵犯公民个人信息罪。所以，考虑到立法原意，应将侵犯公民个人信息罪放在整个涉个人信息犯罪链条上考虑。本罪的法益应包括个人信息之上所承载的隐私利益、人身利益和财产利益。并且，基于法秩序统一原理，本罪的法益应包括个人信息权。然而，必须指出，并非所有违反国家有关规定获取、提供公民个人信息的行为都处于涉个人信息犯罪地下产业链之上，比如APP经营主体未告知用户而收集个人信息，然后将其用于为合法商业目的，这种非法获取行为及其后续处理行为，即使属于前文所述的合理处理行为，也因侵害了知情权，理应被侵犯公民个人信息罪所规制。

综上，侵害公民个人信息罪的法益应被理解为个人信息权或个人信息上承载的人身利益、财产利益、隐私利益。并且，二者之间的关系是非典型性选择关系：只侵害到前者可以构成本罪，但是因为违反国家有关规定的行为必然是侵害个人信息权的行为，所以不侵害前者而只威胁后者的处理行为，显然不构成本罪。只有在侵害到前者且对后者造成威胁时，才该当本罪的构成要件。

（二）侵犯公民个人信息罪复数法益语境下知情同意原则的适用

我国《刑法》中的侵犯公民个人信息罪，主要包括三种行为方式：违反国家有关规定提供、出售、获取。尽管《刑法》第253条之一第3款中，没有规定违反国家有关规定，但是本文认为，应当将“非法”解释为违反国家有关规定。《刑法》第235条之一第1款与第3款法定刑是相同的，这代表两种实行行为的社会危害性程度相同。可以认为，获取与提供（出售是提供的一种情形）行为本身给法益带来的威胁在程度上没有差异，所以非法的解释应当与违反国家有关规定保持一致。而有论者认为，APP经营主体收集用户个人信息违反双方约定的，可认定为非法获取，所以只要违反了有关个人信息知情同意保护的原则性规定，即视为具有刑法所要求的“非法性”[33]（P122）。本文认为，因为《中华人民共和国网络安全法》规定，不得违反法律、行政法规和双方的约定收集、使用个人信息，所以违反约定收集的行为属于违法。因此，该论者对“非法”的解释与本文对“非法”的解释其实不存在差别。

APP经营主体在收集用户个人信息之后，肯定会采取进一步处理，即使收集之后并不使用，但起码收集之后会加以存储，客观上不可能只实施单纯的收集用户个人信息的行为。某些收集行为本身就给用户的法益带来风险，如收集用户通讯录的行为对隐私利益有风险，收集之后的进一步处理行为也可能对其法益造成风险，所以收集行为的风险除了包括收集行为本身的风险之外，还应当包括收集之后的后续处理行为带来的风险。如前所述，完善后的知情同意原则要求，APP经营主体应当在隐私政策中告知可能给用户隐私利益、财产利益、人身利益带来风险的处理行为之风险，所以在征求用户对收集行为之同意的场合，APP经营主体必须在隐私政策中将可能给用户个人信息上承载的法益带来风险的收集行为及其后续处理行为之法益风险全部告知用户。比如，APP隐私政策或许可以按如下方式告知用户法

益风险:“我们请求收集您的**信息,收集该信息时,您的人身利益或隐私利益或财产利益可能遭受**程度的风险,收集后我们打算对其加以**处理,此时您的上述法益可能遭受**程度的风险。”如果用户点击同意,则满足了经完善的知情同意原则之要求,也满足了刑法上的被害人同意对洞察能力之要求。

在《刑法》第253条之一的话语背景下,非法获取的表现之一便是过度收集。一方面,如果过度收集个人信息的行为及其后续处理行为对于个人信息上承载的多重法益没有风险,那么该过度收集行为就只侵害了用户的个人信息权,即根据前置法享有的个人信息不被过度收集的权利。为了个人信息保护与利用的平衡,用户此时应当同意,即应当放弃前置法赋予他的个人信息不被过度收集的权利,即该当构成要件的过度收集行为不具备实质违法性。另一方面,对于会给用户个人信息之上的多重利益造成风险的过度收集行为(本身会造成风险、其后续处理行为会造成风险,或二者兼有),APP经营主体在隐私政策中需要告知过度行为本身和后续处理行为及其对个人信息背后法益的风险。有人可能会质疑,既然被害人同意的洞察能力要求的是被害人对行为人的法益侵害或危殆化行为之法益风险有认识,在过度收集的场合,只需要对过度收集行为及该行为带来的风险有认识即可,不必要求用户对后续处理行为之风险有认识。要求对后续处理行为之风险有认识,是在挑战刑法之因果关系理论。这种疑问显然是忽略了本文研究背后的语境。本文研究的是APP经营主体与用户之间的知情同意,必须意识到,没有一个合法APP经营主体会只实施用户个人信息收集行为。所以如果要求,APP经营主体在对过度收集行为征求同意时,在隐私政策中只告知过度收集行为之风险,显然不利于用户自决权之行使。显而易见,收集之后必然进行进一步处理行为,所以,进一步处理的风险属于收集行为的风险,因此在收集时,应一并告知。

有论者质疑了对违反国家有关规定行为的同意之有效性,认为如果收集、使用个人信息的行为违反了前置性法律法规或部门规章,那么,即便个人信息主体做出同意的意思表示,也不能被认定是有效的,不能排除其刑事违法性[33](P124)。也就是说,对于APP经营主体过度收集或提供的行为,用户不能同意。但本文认为,侵犯公民个人信息罪中的国家有关规定,属于管理性强制性规定,违反该类规定的隐私政策条款确实不合现行法律法规,但是作为合同(隐私政策)相对方的用户对于这类条款可以同意。因为违反《刑法》第253条之一中所谓国家有关规定之行为本身,侵害的只是信息主体的隐私权或一般个人信息权,而不会侵害社会公共利益和国家利益。个人按照自己的意愿处置自己的法益,是个体人格的展开,是实现个体价值的一种途径,刑法应该以一种宽容的态度放松不必要的保护[34](P105)。按照违反现行法律法规的隐私政策实施的过度收集行为,具有现行前置法的违法性。具有前置法违法性的收集行为该当《刑法》第253条之一的构成要件,但是符合改造之后知情同意原则的用户同意是违法阻却事由,因此这种不合规的过度收集行为不构成犯罪。

非法获取的表现之二是,所谓“合法获取,非法滥用”。其中合法获取是指,APP经营主体获得用户对收集行为的同意后,收集了用户的个人信息,而非法滥用是指将该个人信息用于非法目的。就“非法滥用”而言,首先,将“合法获取”的个人信息用于告知以外的目的,此行为未必是非法滥用,因为前文已述,存在合理的个人信息创新性利用行为。其次,给用户本人的隐私利益、财产利益、人身利益带来威胁的基于非法目的而使用的行为(如利用用户个人信息对其进行敲诈勒索、电信诈骗等),是非法滥用。最后,将个人信息用于不利于公共利益的非法目的,属于非法滥用。根据改善之后的知情同意原则,如果用户同意APP经营主体收集其个人信息,则意味着用户同意APP经营主体以特定使用目的,以特定使用方式,在将来的使用会给用户法益造成特定程度风险的情况下收集其个人信息。或者说,用户同意APP经营主体收集其个人信息是有前提条件的,即将来APP经营主体应将其个人信息以告知方式用于告知目的且使用行为只能给用户带来已告知的特定程度之风险(如果不用于告知目的,则创新性目的必须合理合法)。所以,上述“非法滥用”的第二、三种情形,形式上是“合法获取”,但实际并不满足用户同意收集的前提条件,因此构成非法获取公民个人信息,但因为此时用户没有同意收集,故不存在被害人同意

是否是出罪事由之问题。

本文通过列举三种情况，说明用户同意与违反国家有关规定提供个人信息的关系。

假设一：甲APP在隐私政策中告知用户其过度提供个人信息的行为及其风险，用户表示同意。过度提供行为违反了法律规定的个人信息保护之必要性原则，所以属于违反国家有关规定提供，但是如前所述，必要性原则之要求属于管理性强制性规定，违反该规定的合同条款有效，即用户对此的同意有效。所以甲APP的该当构成要件的过度提供行为因用户同意而阻却违法，不构成犯罪。

假设二：甲APP在隐私政策中告知用户对本APP提供的第三方应用乙APP（合法APP）的过度提供行为、甲APP所了解的乙APP保护个人信息的能力、乙APP向甲APP承诺的为了合法运营APP之目的处理个人信息的方式、乙APP的该处理方式可能给用户法益带来的风险，用户点击“我同意”隐私政策，结果乙APP对个人信息的该处理行为侵害了用户个人信息背后的人身、财产、隐私利益。在这种情况之下，因为用户了解且同意甲APP的过度提供行为及其后续风险，因此符合被害人同意成立条件，所以，甲APP的该当构成要件的过度提供行为不具备违法性。乙APP与甲APP实施的都是合法经营行为，只是因为技术水平原因而对用户法益造成侵害，所以乙APP不构成侵犯公民个人信息罪，甲APP也不构成帮助信息网络犯罪活动罪。

假设三：其他条件不变，但乙APP本身是非法APP，以出售为目的获取用户个人信息，但是甲对此不知情，乙在获得甲APP提供的用户个人信息后将其出售给违法犯罪分子（如电信诈骗集团）或乙自己使用这些用户个人信息从事犯罪活动，结果用户法益（人格利益或财产利益）遭受侵害。此时乙APP无疑构成侵犯公民个人信息罪（违反国家有关规定出售），但是甲APP是否是违反国家有关规定提供公民个人信息，这取决于甲APP是否对乙APP的资质进行了审查。如果甲尽到了审查义务后，仍没有发现乙APP的非法性，那么甲提供个人信息给关联方的行为只是技术中立行为，甲不构成违法国家有关规定提供。此时甲不该当侵犯公民个人信息罪之构成要件，因此不必研究用户同意是否是被害人同意之问题。如果甲APP没有尽到对其关联方乙APP业务合法性的审查义务，那么甲APP应被认为明知乙APP业务的非法性，构成非法提供。此时因为在隐私政策中甲APP未能如实告知用户关于乙APP之情况，所以用户对提供行为及其风险的同意无效。因此，甲APP构成乙APP侵犯公民个人信息罪的帮助犯。

五、知情同意原则作为个人信息处理者合规策略之限制

自2017年被称为“企业合规无罪抗辩第一案”的“某巢（中国）有限公司西北区婴儿营养部非法获取公民个人信息案”（甘肃省兰州市中级人民法院[2017]甘01刑终第89号刑事裁定书）终审宣判以来，刑事合规问题便成为国内刑法学研究的热点问题之一。具体到个人信息处理者刑事合规的基本路径，一般认为应通过合规计划的制定和实施，将法律法规赋予的法定义务转化为公司内部制度，实现网络平台内控机制与法律法规尤其是刑法的统一[35]（P98）。但与此同时，对于所有违反国家有关规定的收集与提供公民个人信息的行为，用户同意是否都可以被作为出罪事由？知情同意原则显然不是个人信息处理者滥用个人信息的避风港，也并非所有处理行为都要征得信息主体的同意，即知情同意原则的功能需要受到限制。

（一）知情同意原则的消极限制

有论者认为，不能简单地以知情同意原则作为任何情况下不当收集个人信息的合格抗辩，知情同意原则不是万能法则，需要受到四方面的限制。首先，其作为一种实现经济利益的手段，不能与宪法保护的人格利益的通信自由、通信秘密相抗衡。其认为，通讯录、通话记录与短信内容属于通信秘密和通信自由之客体。其次，从《民法典》的体系安排上可以看出，人格尊严是法律保护的更高价值，优先于财产利益和私法自治的价值，而私密信息所蕴含的人格权益高于财产权益，所以作为实现经济利益的手段，知情同意原则不能用来限制作为具体人格权的隐私权。涉嫌侵害个人私密信息的行为，只有在既满足

个人信息权益抗辩,又满足隐私权侵权抗辩的情况下,才能够免责。再次,知情同意原则应受其他个人信息保护原则的制约,即正当目的原则和必要原则。最后,知情同意原则要受到诚实信用原则和公序良俗原则的限制[16](P12-14)。本文支持同意原则不是万能的观点,但认为侵犯国家社会利益和违反公序良俗原则构成对同意原则的限制,不认为必要原则以及目的限制原则可以限制同意原则的出罪功能。

首先,对于必要和目的原则,必须认识到违反必要原则或目的限制原则的经同意的处理行为,只是因违反了管理性强制性规定而具有行政违法性或民事违法性,并不具备刑事违法性。也就是说,在《民法典》或《个人信息保护法》中,同意确实无法成为违反必要原则和目的限制原则的行为的违法性阻却事由,但是同意是违反行政法或民法中此类行为的出罪事由。因为对于违反管理性强制性规定的条款,同意是有效的,而用户一旦同意,即代表其放弃了个人信息不受过度处理的个人信息权,自然不具备刑法上的实质违法性。必要原则和目的限制原则本身是否具有存在的必要,值得怀疑。必要性原则是指,只能收集实现隐私政策中所表明的目的所必要的最小数据量。目的限制原是指未经新的同意,不得将数据用于其他不相关的目的。在大数据时代不宜继续将这两个原则作为数据处理准则,而应以是否对个人信息背后的人身、财产、隐私利益造成不合理风险为依据,来决定是否用前置法规制 APP 经营主体处理用户个人信息之行为。如上所述,过度处理行为以及创新性处理行为可能是合理处理行为,但是按现行法律规定,这种有利于企业或社会且不会危及个人信息法益的处理行为,却具备行政违法性或民事违法性。近来我国国家工业和信息化部、多个地方性通信管理局频繁责令过度收集个人信息的 APP 整改,并对规定期限内未完成整改的 APP 予以下架处理,可是这种看似重拳出击的执法活动真的有必要吗?尤其是,如果过度收集的个人信息只是被用于为本企业合法经营决策提供依据,是否有必要打击?本文认为,以必要原则为主要执法依据而开展的对 APP 收集个人信息加以整治的活动有些矫枉过正,是在对个人信息权进行过度保护,而严重限制了 APP 经营主体开发或改善合法业务,不利于营造保护中小微型企业发展的营商环境。综上,必要原则以及目的限制原则不会也不应成为用户同意原则发挥出罪功能的障碍。

其次,对于违反公序良俗原则或侵犯国家社会利益的处理行为,因为国家社会利益或秩序不是用户个人能处分的法益,所以用户的同意是无效的,所以这两个事由理应构成对同意原则出罪功能的限制。

再次,对于隐私权以及作为宪法权利的通信自由与通信秘密,本文认为仍属于用户可以自由处分的权利①,所以如果处理用户个人信息的行为给用户本人的隐私权或通信自由、通信秘密造成不合理风险,只要用户对 APP 经营主体在隐私政策中告知的此风险表示同意,则同意仍可以成为出罪事由。

(二)知情同意原则的积极限制

所谓同意原则的积极限制是指,有些个人信息处理行为不需要经过用户同意。处理个人信息的行为的合法性要素不仅包括知情同意,欧盟《一般数据保护法案》(GDPR)规定了其他五种,即处理数据是为签订或履行合同之必要;处理数据是为遵守法律义务之必要;处理数据是为了保护数据主体或其他自然人的切身利益;处理数据是为了公共利益或行使公务职权;处理数据是为了追求数据控制者的合理利益,但不得损害数据主体的利益。这些合法性要素只需满足其一,处理行为即为合法,侵犯公民个人信息罪不成立。因而同意原则并非本罪唯一出罪事由,上述其他合法性要素都是本罪的出罪事由。我国《民法典》也规定了处理个人信息不承担民事责任的情形,即合理处理已经公开的个人信息,且信息主体未明确拒绝、该处理也未侵害其重大利益;维护公共利益或该自然人合法权益的合理处理行为。我国《个人信息保护法》也规定了除同意之外,个人信息处理行为的合法事由:为订立或者履行个人作为一方

① 通讯录除外。不存在没有通讯录就不能提供的互联网移动应用服务,且自然人的通讯录不仅是该自然人的个人信息,也是其通讯录中好友的个人信息。如果 APP 经营者处理某用户的通讯录的行为给其通讯录中好友的隐私利益带来了不合理的风险,那么显然该用户的同意是没有意义的。

当事人的合同所必需；为履行法定职责或者法定义务所必需；为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需；依照本法规定在合理的范围内处理已公开的个人信息；为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息；法律、行政法规规定的其他情形。

由此可见，未经用户同意，个人信息处理未必违反前置性法律，此时处理行为不满足侵犯公民个人信息罪的构成要件，进而无讨论用户同意是否是出罪事由之必要。其实，上述除同意之外的合法化事由，与本文前述合理的个人信息处理行为不谋而合。“为订立或者履行个人作为一方当事人的合同所必需”的处理行为，一般不会给用户隐私利益、财产利益、人身利益带来风险，即使带来风险，这种风险也是合理的，是大数据时代必然会出现的，是用户应当容忍的。欧盟《一般数据保护法案》（GDPR）明确要求，处理数据是为了追求数据控制者的合理利益，但不得损害数据主体的利益。这几乎与本文对合理处理行为的界定完全一致，而这也是在大数据时代，为了促进个人数据的开发与利用，用户有义务同意的，因而不需征求其同意。

个人信息利用与保护之间的平衡是大数据时代永恒的课题。本文择取个人信息保护与利用这一维度，以APP经营主体为例，对个人信息处理者的刑事合规与个人信息保护，提出了两条解决路径，即合理的个人信息处理行为只需告知而不需获得用户同意，借此保障个人信息处理者对个人信息的利益期待；对个人信息附着的隐私、人身、财产利益有风险的处理行为必须征得用户同意，借此保障用户的个人信息自决权以及对个人信息背后法益的自决权。

参考文献

[1] 叶名怡.论个人信息权的基本范畴.清华法学,2018,(5).
[2] 程啸.我国《民法典》个人信息保护制度的创新与发展.财经法学,2020,(4).
[3] 范为.大数据时代个人信息保护的路径重构.环球法律评论,2016,(5).
[4] 张新宝.论个人信息权益的构造.中外法学,2021,(5).
[5] 王叶刚.论网络隐私政策的效力——以个人信息保护为中心.比较法研究,2020,(1).
[6] 万方.网站隐私声明的效力与解释规则.北外法学,2019,(2).
[7] 阳雪雅.论企业违反网络隐私政策的违约责任适用.法学论坛,2021,(5).
[8] 李延舜.我国移动应用软件隐私政策的合规审查及完善——基于49例隐私政策的文本考察.法商研究,2019,(5).
[9] 高富平.个人信息保护：从个人控制到社会控制,法学研究,2018,(3).
[10] 王利明.合同法新问题研究.北京：中国社会科学出版社,2011.
[11] 齐爱民.信息法原论——信息法的产生与体系化.武汉：武汉大学出版社,2010.
[12] 陆青.个人信息保护中“同意”规则的规范构造.武汉大学学报(哲学社会科学版),2019,(5).
[13] 范海潮,顾理平.探寻平衡之道：隐私保护中知情同意原则的实践困境与修正.新闻与传播研究,2021,(2).
[14] 吕炳斌.个人信息保护的“同意”困境及其出路.法商研究,2021,(2).
[15] 蔡星月.数据主体的“弱同意”及其规范结构.比较法研究,2019,(4).
[16] 张新宝.个人信息收集：告知同意原则适用的限制.比较法研究,2019,(6).
[17] 万方.隐私政策中的告知同意原则及其异化.法律科学,2019,(2).
[18] 陈瑞华.企业合规基本理论,北京：法律出版社,2020.
[19] 金日秀,徐辅鹤.韩国刑法总论.郑军男译.武汉：武汉大学出版社,2008.
[20] 蔡颖.被害人同意与被害人自陷风险的统合——以刑法中被害人同意的对象为视角.法学评论,2021,(5).
[21] 孙国祥.民法免责事由与刑法出罪事由的互动关系研究.现代法学,2020,(4).
[22] 刘艳红.民法编纂背景下侵犯公民个人信息罪的保护法益:信息自决权——以刑民一体化及《民法总则》第111条为视角.浙江工商大学学报,2019,(6).
[23] 乌尔斯·金德霍伊泽尔.刑法总论教科书.蔡桂生译.北京：北京大学出版社,2015.

[24] 关哲夫.讲义·刑法总论.东京:成文堂,2015.
[25] 张明楷.刑法学.北京:法律出版社,2016.
[26] 车浩.论被害人同意的体系性地位——一个中国语境下的“德国问题”.中国法学,2008,(4).
[27] 王钢.被害人承诺的体系定位.比较法研究,2019,(4).
[28] 于冲.侵犯公民个人信息罪犯罪圈的“收缩”与出罪化路径.青海社会科学,2021,(1).
[29] 喻海松.侵犯公民个人信息罪司法解释理解与适用.北京:中国法制出版社,2018.
[30] 迟大奎.作为抽象危险犯的侵犯公民个人信息罪之检视.湖北社会科学,2019,(11).
[31] 江海洋.侵犯公民个人信息罪超个人法益之提倡.交大法学,2018,(3).
[32] 凌萍萍,焦治.侵犯公民个人信息罪的刑法法益重析.苏州大学学报(哲学社会科学版),2017,(6).
[33] 张勇.APP个人信息的刑法保护:以知情同意为视角.法学,2020,(8).
[34] 车浩.自我决定权与刑法家长主义.中国法学,2012,(1).
[35] 李本灿.刑事合规理念的国内法表达——以“中兴通讯事件”为切入点.法律科学(西北政法大学学报),2018,(6).

The Decriminalized Function of "Informed Consent Clause" In the *Personal Information Protection Law*

Li Lifeng (Jilin University)

Abstract The principle of informed consent as specified in the *Personal Information Protection Law* is an important embodiment of the preventive personal information protection mechanism. Taking the personal information processing subject represented by APP as an example, the privacy policy on the basis of reasonably improving the principle of informed consent can be regarded as the agreement between the personal information processor and the personal information subject, which could also be regarded as the substantial agreement with the victim's consent in the criminal law. In the context of criminal compliance, the personal information processor should adjust the privacy policy text to protect the user's right to know. For the processing behavior that will bring risks to the multiple legal interests behind personal information, the user must be informed of the behavior and the accompanying risks and be asked for his/her consent so as to complete the transformation from the simple principle of personal information protection to the principle of balance between personal information protection and utilization. The improved informed consent clause can be consistent with the victim's consent principle and help personal information processors avoid criminal responsibility for infringing on citizens' personal information.

Key words *Personal Information Protection Law*; privacy policy; the principle of informed consent; the decriminalized cause of the crime; criminal compliance of infor provider; cyber crime; right to self-determination of personal information; APP

■ **收稿日期** 2021-08-01
■ **作者简介** 李立丰,法学博士,吉林大学法学理论研究中心教授,吉林大学法学院教授、博士生导师;吉林 长春 130012。
■ **责任编辑** 李 媛