法商研究 Studies in Law and Business
Vol. 39 No. 5(2022)

三重授权原则在个人信息处理中的限制适用

向 秦*

摘 要:三重授权原则实为“用户同意+平台授权+用户同意”,是对《中华人民共和国个人信息保护法》第23条个人信息提供的典型描述,是在具体个案中第三方数据获取行为是否构成不正当竞争这一特定法律后果的裁判规则,其适用应受到合理限制。在主体上,第23条的“提供方”为非国家机关处理者或国家机关处理者;三重授权的“平台方”限于非国家机关处理者。在客体上,第23条适用于“处理的个人信息”;三重授权限于平台方生产并享有财产性权益的个人数据集合与个人数据报告。在场景上,第23条适用于“向其他个人信息处理者提供(共享和转让)”;三重授权限于开放平台模式的数据共享。在法律后果上,“同意”不等于“授权”,未经三重授权不一定侵权,经三重授权也不绝对免责,用户同意与平台授权有条件地相互替代。

关键词:个人信息 三重授权原则 不正当竞争

个人信息以0和1比特形式在不同信息处理者之间传输与流动,形成“个人—信息处理者—其他信息处理者”多元关系。为了平衡各方利益,法官在我国企业数据权益纠纷中构建了控制格局下的数据共享模式:三重授权原则。第三方通过平台方获取正常经营范围所需用户数据时,[①]平台方须经用户授权,第三方既须经平台方授权也须经用户重新授权。该模式是同意规则在个案中的延伸,被视为第三方数据获取行为正当性的检验标准,违反该规则便是违背商业道德,依据《中华人民共和国反不正当竞争法》(以下简称《反不正当竞争法》)第2条(“一般条款”)的规定构成不正当竞争。[②] 因此,三重授权原则成为实践中平台方的诉讼利器,第三方则根据信息可携理论以“用户已同意”为由抗辩。然而场景主义规制下不足以形成确定、稳定和统一的裁判规则,[③]难谓三重授权乃普适规则。“一般条款”的内在模糊性决定其适用的严重不确定性,三重授

* 上海交通大学凯原法学院数据法律研究中心研究人员
基金项目:国家社会科学基金重大项目(18ZDA145)

① 用户数据是指个人信息处理者在各种场景中采取技术手段获取的用户相关信息的总和,以电子为表征形态。参见彭诚信、向秦:《“信息”与“数据”的私法界定》,《河南社会科学》2019年第11期。

② 参见王燃:《论网络开放平台数据利益分配规则》,《电子知识产权》2020年第8期。

③ 参见杨贝:《个人信息保护进路的伦理审视》,《法商研究》2021年第6期。

权不必然成为一般条款的判断标准。[①] 若不加分析地将这一规则直接适用在所有场景的平台数据获取案件中,则严格的数据获取要求不仅保护信息主体利益效果有限,而且难以维护自由竞争的环境,可能限制数据的流转与开发。

《中华人民共和国个人信息保护法》(以下简称《个人信息保护法》)第 23 条对"向其他个人信息处理者提供其处理的个人信息"作出立法回应,与三重授权原则一起,构成处理者之间用户数据流动规则的"一体两面",即一方直接提供数据与另一方间接获取数据。因为单个主体掌握有限的数据资源,其有通过市场化或非市场化方式获取他人数据资源的主动需求,也有作为持有者对外提供、分享的被动需求。通过成文规范与裁判规则的解释与互动,对三重授权原则的适用类型化和要件化,将有助于人民法院做出实现最佳市场竞争效果的正当评判。按照"新二要素说",规则的逻辑结构包括构成要件和法律后果。[②] 本文基于这一思路,在分析正当性基础上,合理限制三重授权原则适用的行为模式及法律后果,以实现逻辑自洽并指导实践。

一、三重授权原则的提出与正当性评价

(一)三重授权原则的司法运用

为获取更多的竞争优势,处理者不再囿于从自身产品或服务中获取用户数据,而是积极寻求第三方数据来源。国内目前典型的数据权益纠纷发生在非法获取其他平台持有的数据这一类案件中,2016 年"微博诉脉脉案"[③]针对第三方通过开放平台接口获取用户数据提出三重授权原则,在个人信息流动、易手等再利用环节给予用户、持有者(微博)受保护及控制的权利,限制第三方(脉脉)超出授权范围获取平台用户数据。2018 年"淘宝诉美景案"[④]采用"三重授权许可使用规则",在将用户行为痕迹信息认定为非个人信息的同时又参照个人信息的保护对用户行为痕迹信息进行保护,从而将三重授权原则的适用范围,扩张至"使用其他网络运营者收集的用户信息"的宽泛场景。2019 年"微信诉抖音、多闪案"[⑤]将三重授权原则定位为开放平台模式下经营者应遵循的商业道德,与"合法、正当、必要"原则并列,进一步限制第三方非法获取其他平台持有的数据。至此,三重授权原则成为评判第三方数据获取行为是否具有"不正当性"的默认行业标准。

在上述裁判文书未对三重授权原则的适用给出充分理由的情形之下,学界对三重授权究竟是"哪三重"在认识上也存在分歧。第一种解读是用户对平台方收集行为授权,平台方将收集的信息分享给第三方须用户授权,被共享方获取前述信息也要用户授权。[⑥] 该观点是基于《中华人民共和国民法典》(以下简称《民法典》)第 1038 条"未经被收集者同意,不得向他人非法提供其个人信息"的规定对收集和后续利用行为的正当性分开评价,属于传统知情同意。第二种解读是平

① 参见黄细江:《涉企业数据竞争行为的法律规制》,《知识产权》2021 年第 2 期。

② 参见雷磊:《法律规则的逻辑结构》,《法学研究》2013 年第 1 期。

③ 参见北京市海淀区人民法院 2015 年海民(知)初字第 12602 号民事判决书、北京知识产权法院(2016)京 73 民终 588 号民事判决书。

④ 参见杭州铁路运输法院(2017)浙 8601 民初 4034 号民事判决书、浙江省杭州市中级人民法院(2018)浙 01 民终 7312 号民事判决书。

⑤ 参见天津市滨海新区人民法院(2019)津 0116 民初 2091 号民事裁定书。

⑥ 参见王利明:《数据共享与个人信息保护》,《现代法学》2019 年第 1 期。

台方收集用户数据须经其授权，第三方获取前述数据须平台授权和用户授权。[①] 该观点将收集时的同意视为不同处理活动混在一起的概括同意。第三种解读是个人信息收集和利用均应取得“用户授权＋平台授权＋用户授权”，即平台收集和向第三方分享须充分告知并经用户授权，第三方获取和利用前述数据既要平台授权也要用户再次明确授权。[②] 第三种解读更符合判决书原文，即“数据提供方向第三方开放数据的前提是数据提供方取得用户同意”（授权 I）和“第三方平台在使用用户信息时还应当明确告知用户其使用的目的、方式和范围，再次取得用户的同意”（授权 III）及“在实施开放平台战略中，有条件的向开发者应用提供用户信息……新浪授权……维护企业自身的核心竞争优势”（授权 II）。

授权 I 是平台方、第三方行为正当性的前提，不能倒置，只能在授权 II 和授权 III 之前。未经用户同意的平台方处理行为本身可能因欠缺合法性而无权向第三方分享用户数据。授权 II 和授权 III 并非递进关系，第三方可同时获得用户与平台授权。授权 II 意味着司法裁判以平台控制并持续积累用户数据资源的现实为逻辑起点，认可其作为用户数据经济利益的生产者而单独或共同享有财产性权益。第三方因与平台事前订立“开发者协议”实现用户数据合法传输，该协议的内容由平台方制定，效力得到判决普遍承认而成为数据共享基本规则。授权 III 是尊重用户对个人信息权益的行使和新技术的选择，用户授权基础是个人信息上的主体权益，该权益既是一种宪法层面的人权，也是落实到私法层面的人格权益。第三方因用户再次授权而具备用户层面的正当性。三重授权模式是以裁判规则形式践行《全国人民代表大会常务委员会关于加强网络信息保护的决定》《中华人民共和国消费者权益保护法》《中华人民共和国网络安全法》（以下简称《网络安全法》）等标志性立法所确立的收集、使用个人信息须征得主体同意的基本规则，从形式上看具有合法性。

（二）三重授权原则的正当性评价

三重授权原则从诚信原则发展而来，成为具有一定约束力的个案规范。个案规范是解决具体个案的权宜之策而非普适性规范，但若对其后相同或相似案例产生法律拘束力，便成为“法官造法”即判例。[③] 我国虽然不存在判例法的法律形式，但是由最高司法机关选择、确认和公布的典型判例，在司法实践中起到了法的渊源的作用。在“微博诉脉脉案”中脉脉因超出授权范围获取用户数据违反了诚信原则和商业道德而败诉。法官仰赖边界模糊的商业道德保护条款（《反不正当竞争法》第 2 条、第 12 条）审理数据权益纠纷，并提炼出“三重授权”。在随后的判决中，该原则本身被视为一项商业道德，违背三重授权等同于违背商业道德，构成不正当竞争。

赞同者认为三重授权保护思路“对于我国未来个人信息保护以及数据信息产业的健康发展具有指导意义”。[④]中立者认为三重授权是一种“高标准、严要求”，为用户和企业提供较强保护，

① 参见李安：《人工智能时代数据竞争行为的法律边界》，《科技与法律》2019 年第 1 期；戴昕：《数据界权的关系进路》，《中外法学》2021 年第 6 期。

② 参见薛军：《大数据时代数据信息权益的法律保护》，《中国知识产权报》2017 年 2 月 8 日；徐伟：《企业数据获取“三重授权原则”反思及类型化构建》，《交大法学》2019 年第 4 期；刁云芸：《涉数据不正当竞争行为的法律规制》，《知识产权》2019 年第 12 期；周学锋：《网络平台对用户生成数据的权益性质》，《北京航空航天大学学报》（社会科学版）2021 年第 4 期。

③ 参见彭诚信：《从法律原则到个案规范——阿列克西原则理论的民法应用》，《法学研究》2014 年第 4 期。

④ 薛军：《大数据时代数据信息权益的法律保护》，《中国知识产权报》2017 年 2 月 8 日。

但在多数个人信息处理情境中并不适合。[①] 反对者认为三重授权无法适应场景理论下用户数据差异化保护需要,不符合效益决策模型,[②]不利于技术创新,缺乏实质意义。[③]笔者认为,脱离特定案件中用户数据自身可识别性、平台市场地位等因素差异而普遍适用三重授权是值得质疑的。只有在部分情境中合理限制适用才具有正当性,否则极易抑制"好人"第三方的创新与社会福利总量增加。一方面,商业道德的模糊性易造成自由裁量权被滥用。换言之,脱离法定类型的不正当竞争行为而视三重授权为商业道德,直接适用的究竟是公认商业道德,还是占据市场强势地位的平台主导下的行业潜规则。[④] 另一方面,平台存在借保护用户之名,行限制竞争对手之实的可能性。[⑤] 平台方虽以用户隐私受到极大威胁为由要求司法机关认可其控制权,但也可能是出于对数据资源封锁限制目的而寻求权力,在数据驱动市场中的主体缺乏自愿开放与分享数据的动机,在实践中不乏第三方宁愿违法也要突破平台设置的共享壁垒的案例。

但要承认的是,在鼓励数据开放的前提下,适当对第三方处理行为苛以更高的正当性标准,优势是在部分情境中既能加强对用户利益和平台方投资预期的合理保护,也能兼顾其他处理者参与数据竞争的合理需求。回应"哪些情境适用"才是反思三重授权的核心。(1)从社会价值实现角度看,三重授权是对用户数据上多元利益产权配置的具体尝试。考虑到现阶段数据社会化利用的实际需求,不应由单一主体独自排他地享有数据资产剩余控制权,而应以个人信息社会价值实现为目标,使每个主体参与数据生产和利益分配。此外,数据提供方在其他利用场景中也是需求方,上游环节的平台方与下游环节的第三方的地位随着场景不同而互换,秉持这样的"同理心"来建立安全的商业秩序有利于整个数据产业链的发展。[⑥] (2)从数据共享关系角度看,三重授权有助于稳定、长期、可信任的数据开放与共享关系的建立。对于用户,平台授权为其多添加一道保护屏障。提供重要平台服务的处理者通过履行"守门人"义务(《个人信息保护法》第 58 条)以拒绝对用户权益有潜在重大威胁的第三方。[⑦] 对于平台方,平台授权维护其自身竞争优势。对于第三方,用户重新授权是司法实践对信息可携权的有益尝试,体现出间接避免平台垄断数据之可能性。从长远看,维护各方安全感才能反过来促进数据共享意愿,保护共享意愿就是保护信任。(3)从与成文规范的互动看,三重授权与《个人信息保护法》第 23 条的内在逻辑一致,均以平台控制为起点。平台授权之所以成为必要一环,是因为在数据流动与连续易手过程中,个人对信息的控制受到极大的限制,掌握技术与设备的平台是用户数据的实际控制者。为了避免用户对个人信息控制能力实际丧失所带来的危害,判决确认平台对用户数据享有控制权,以实现保护个人信息之目的。第 23 条在此基础上更加强化平台控制,只要接收方在"原先的处理目的、处理方式"范围内便无须再次征得用户同意。按照规则适用对象不同,第 23 条是约束一般行为人的行为规则,三重授权原则是判定是否构成不正当竞争这一特定法律后果的裁判规则。个人信

① 参见徐伟:《企业数据获取"三重授权原则"反思及类型化构建》,《交大法学》2019 年第 4 期。

② 参见许娟:《互联网疑难案件中数据权利保护的风险决策树模型》,《南京社会科学》2019 年第 3 期。

③ 参见刘继峰、曾晓梅:《论用户数据的竞争法保护路径》,《价格理论与实践》2018 年第 3 期。

④ 参见叶明、郭江兰:《误区与纠偏:数据不正当竞争行为认定研究》,《西北民族大学学报》(哲学社会科学版)2019 年第 6 期。

⑤ 参见肖梦黎:《平台型企业的权力生成与规制选择研究》,《河北法学》2020 年第 10 期。

⑥ 参见王磊:《个人数据商业化利用的利益冲突及其解决》,《法律科学》(西北政法大学学报)2021 年第 5 期。

⑦ 参见田小军、曹建峰、朱开鑫:《企业间数据竞争规则研究》,《竞争政策研究》2019 年第 4 期。

息提供方和接收方应遵守第23条的行为规范及其约束效果，提供方应当履行告知义务并就向他人提供这一处理行为取得个人单独同意，接收方应在已经取得同意的范围内处理。违反第23条的行为人可能承担包括行政处罚、治安管理处罚或因侵害用户个人信息权益而承担侵权责任乃至刑事责任等多种不利后果。当某个特定行为类型出现后，裁判者根据三重授权判断第三方行为是否因欠缺正当性构成不正当竞争，侧重于法律上的评价性后果，第三方可能承担损害赔偿责任以维护平台方的数据财产性权益与竞争优势。

二、三重授权原则的构成要件

场景完整性理论是指个人信息后续处理应受最初信息收集时的场景限制，且当个人信息处理目的、方式发生变化时，场景随即改变。[①] 也即个人信息处理规则是在不同场景中设定的，不同场景由不同法律关系决定。以下结合场景理论与《个人信息保护法》第23条，从主体、客体、场景来厘清三重授权的适用范围。

（一）适用主体

《个人信息保护法》第23条采用“个人”“个人信息处理者（提供方）”“其他个人信息处理者（接收方）”来描述个人信息提供关系中的主体。与三重授权相关判决中的“用户”“平台方”“第三方”对照。（1）“个人”和“用户”均限于自然人，不包括法人和非法人组织。根据现行法律法规，法人和非法人组织享有名称权、名誉权和荣誉权（《民法典》第110条），自然人的个人信息受法律保护（《民法典》第111条）。可见，企业法人信息，法律上仅禁止未经允许冒用其名称的行为，企业并非个人信息权益主体。“城市链接诉企查查案”[②]判决明确否定了企业法人作为个人信息权益主体的地位。（2）“个人信息处理者（提供方）”既可为商业领域提供个人信息的非国家机关处理者，也包括公共管理领域共享个人信息的国家机关处理者；“平台方”仅限于非国家机关处理者，也是个人信息控制者，是与信息主体直接相对的义务主体。尽管我国对国家机关与非国家机关处理个人信息采用统一立法模式，但是两者的个人信息处理行为具有差异性。平台方、第三方与用户是平等主体间的法律关系，处理个人信息多为开展经营活动所需，无其他合法事由时须用户同意。国家机关与个人是不平等主体间的法律关系，处理目的是履行法定职责而非营利，是维护社会秩序、公共利益及国家利益所需，在绝大多数情况下无须个人同意。（3）“其他个人信息处理者（接收方）”和“第三方”均为个人信息处理者。《个人信息保护法》第23条经历了从“第三方”到“他人”到“其他个人信息处理者（接收方）”的立法修订过程，这一立法技术并非偶然。“其他个人信息处理者（接收方）”的表述更精确，更符合第23条的立法目的，否则无法与涉及多个处理者的其他场景区分。第一，接收方只能在一定目的及范围内处理个人信息，意味着接收方是特定的，不同于公开披露所涉及的社会或不特定人群（《个人信息保护法》第25条）。第二，接收方不同于委托处理信息中的“受托方”，在委托合同不生效、无效、被撤销或者终止后，受托方要返还或删除个人信息，不得私自保留，而接收方不必负有返还或删除义务（《个人信息保护法》第21条）。第三，接收方不同于因合并、分立等接收个人信息的“承继方”，承继方应继续履行之前主体的权利

① See Helen Nissenbaum, Privacy in Context, Stanford Law Books, 2010, p.129.

② 参见北京互联网法院（2020）京0491民初10214号民事判决书。

义务,而接收方并非对前一主体个人信息的承继(《个人信息保护法》第 22 条)。第四,接收方不同于共同处理个人信息中的另一方,因为后者的处理目的和方式是由双方共同决定,而非各自自主决定的(《个人信息保护法》第 20 条)。

(二)适用客体

1.数据生产理论下平台数据类型的划分。受欧盟数据法的影响,我国亦倾向于采用个人数据与非个人数据的二分法。① 除个人数据外就是非个人数据。然而,被忽略的事实是:数据是动态的! 二分法的前提是某一类数据的边界清晰,但在实践中个人数据与非个人数据之间几乎没有明确的界限,在技术上可从非个人数据重新识别特定个人,很难保证匿名化、脱敏化处理后的数据一直是非个人数据,故非个人数据也是动态概念,由个人数据范围的扩展与压缩决定。对个人数据的关注不应停留在收集阶段,而应从收集转移到使用,根据实际识别的可能性、易用性和成本提供不同强度的保护。因此,平台数据类型的划分应将个人数据视为一个连续概念,置于"一次利用"到"二次利用"的生命周期中、"收集+存储"到"汇集+分析"加工处理的数据生产过程中,结合数据来源、数据规模、利益主体等多元分类标准划分。第一类是经"收集+存储"得到的"原始数据",包括(单个)个人数据、(单个)非个人数据。(单个)个人数据是特定用户个人信息的电子化转换,来自用户主动提供与共享,用户是(单个)个人数据的生产者,如在"微信诉抖音、多闪案"中抖音应用程序通过第三方登录获取特定用户的昵称、头像等单个个人信息。(单个)非个人数据是来自传感器或工业数据等与用户无关的平台自采的非个人数据,如在"谷米诉元光案"②中谷米平台自采的公交车实时位置等数据。第二类是经"汇集+分析"加工处理后得到的"衍生数据"。衍生数据是由处理者在原始数据基础上加工而成的,处理者是衍生数据的生产者,享有"数据生产者权利"。③ 一种是通过"汇集"形成的规模化数据集合,包括个人数据集合、非个人数据集合。个人数据集合又分为免费或付费直接租用平台原始数据源的平台接口调用模式(如开放平台)与经纪商向客户提供某一主题的数据文件集模式。④ 数据集合往往被认定为经平台多年积累而成的商业资源,如在"大众点评诉百度案"⑤中百度通过搜索技术抓取并大量全文展示来自大众点评网的信息。另一种是通过"分析"形成的具有预测、识别、知识等价值的个人数据报告与数据产品,区别在于是否包含识别性的个人信息内容。例如,个人信用报告既包含用户信用信息也有平台方分析加工的劳动投入,属于个人数据报告;在"淘宝诉美景案"中"生意参谋"则是经特定算法通过深度分析过滤、提炼整合等处理后形成的不包含个人数据但具有预测功能的数据产品。

2.适用三重授权原则的平台数据类型及其正当性。《个人信息保护法》第 23 条适用于"处理的个人信息",不同于该法第 4 条中的"个人信息",处理意味着至少经过了"收集"。故第 23 条适用客体可涵盖平台所有 4 类数据:(单个)个人数据、个人数据集合、个人数据报告、非个人数据

① 参见程啸:《论大数据时代的个人数据权利》,《中国社会科学》2018 年第 3 期。

② 参见广东省深圳市中级人民法院(2017)粤 03 民初 822 号民事判决书。

③ See Laura Somaini, Regulating the Dynamic Concept of Non-personal Data in the EU: From Ownership to Portability, 6 European Data Protection Law Review, 84 (2020).

④ 参见高富平:《数据生产理论——数据资源权利配置的基础理论》,《交大法学》2019 年第 4 期。

⑤ 参见上海市浦东新区人民法院(2015)浦民三(知)初字第 528 号民事判决书、上海知识产权法院(2016)沪 73 民终 242 号民事判决书。

(单个、集合、数据产品)。第23条作为一般行为规则,宽泛的客体范围为司法适用留下解释空间,但作为更严格限制数据获取的三重授权的客体却不宜过于宽泛。(1)第三方获取非个人数据(单个、集合、数据产品)时,仅要"平台授权",不适用三重授权。该类数据与个人无关或关联识别特定自然人的可能性较低,无须用户同意。在"余某诉酷车易美案"①的二手车辆交易场景中,案涉车况信息经脱敏处理,与其他信息结合关联识别出原告的可能性较低而被认定为非个人信息,未经原告同意不构成侵权。平台方对该类数据享有财产性权益,须经平台授权后处理。"淘宝诉美景案"判决虽没有直接承认淘宝公司对数据产品享有专有财产权,但承认其享有独立的"竞争性财产权益"。(2)第三方获取(单个)个人数据时,经用户同意具有正当性,三重授权简化为"双重授权"。特定自然人的个人数据本质是个人信息,是天然内置财产属性的人格权益。② (单个)个人数据的来源者和生产者是特定用户,对社会的价值贡献仍未脱离用户信息所包含的资讯内容。平台虽付出了一定的劳动收集和存储,但并未提升信息的质量,仅在用户同意范围内依其与用户的约定享有有限使用权。"腾讯诉搜道案"③判决认定第三方未经许可擅自获取他人控制的单一原始数据一般不构成侵权行为,控制者无赔偿请求权。(3)第三方获取个人数据集合时,可适用三重授权。处理者对用户提供的非结构化数据整理汇集"粗加工"使之成为用于分析的对象,个人数据集合因处理者的生产而具备"添附价值"。但个人数据集合因缺乏独创性要件难以纳入知识产权范畴。欧盟以邻接权来保护这类数据库,强调数据的结构化,我国司法实践则以有限排他权来实现与欧盟类似的保护效果,强调平台方有实质性投入和一定数据量。平台方对个人数据在集合整体上享有合法权益,出于对其汇集等成本的认可,是一种与绝对财产权相较而言更弱的保护,故未经许可不得向他人提供平台的个人数据集合。"微信诉抖音、多闪案"判决认定抖音应用程序将其来源于微信开放平台的用户头像、昵称等数据集合提供给多闪应用程序使用,损害了微信及用户的合法权益。(4)第三方获取个人数据报告时,可适用三重授权。个人数据报告由处理者在原始数据上分析加工而成,包括个人信用报告、个人健康评估报告、个人资产状况表、个人职业能力评估等。个人数据报告仍有可识别性,与用户人格利益相关,平台对报告添加了分析劳动,与平台财产性利益相关,由用户与平台方共有。平台对报告享有财产性利益不以独创性为必要条件,根据"额头出汗原则"④即使不具有独创性也可因其劳动和加工创造添加了新内容而享有利益。

3.平台数据开放程度对第三方行为正当性的影响。公开数据与非公开数据的区分取决于用户和平台方是否以设定访问权限或保护技术手段等措施来限制第三方访问。非公开数据的可访问程度因适用不同的限制措施而不同。当平台方通过登录规则或其他措施设置访问权限及用户

① 参见广州互联网法院(2021)粤0192民初928号民事判决书。

② 参见向秦、高富平:《论个人信息权益的财产属性》,《南京社会科学》2022年第2期。

③ 参见杭州铁路运输法院(2019)浙8601民初1987号民事判决书;浙江省杭州市中级人民法院(2020)浙01民终5889号民事判决书。

④ "额头出汗"(sweat of the brow)为早期版权法中大多为信息性或事实性客体所适用的原则,这类客体的创作需要作者付出艰辛劳动和大量投资但其社会价值又决定了原创性的缺乏,因此付出劳动本身就可构成客体获得保护的正当理由,犒赏的是作者的劳动。尽管该原则在版权理论中逐渐淡出,但是对于平台数据权益配置仍有启发意义。参见卢海君:《论作品的原创性》,《法制与社会发展》2010年第2期。

自己设置限制访问时,如“微博诉蚁坊案”[①]第三方须登录后才可查看或即使登录后亦不可查看的新浪微博,往往包含用户私密信息(如用户设置仅自己可见的微博)或不希望他人获取的信息(如用户发布后自行删除的)。第三方未经同意处理可能侵害用户合法权益,可适用三重授权。当平台方采取保密技术手段保护存储在计算机信息系统的数据时,第三方未经授权访问计算机属于“黑客”行为,可同时构成不正当竞争与刑事犯罪。在“谷米诉元光案”中被告同时构成非法获取计算机信息系统数据罪和非法占用他人无形财产权益的不正当竞争行为。当用户对信息特别加密时,第三方未经同意获取涉及侵害隐私权。

公开数据是指用户和平台方均未设定访问权限,如第三方在未登录状态下即可查看的新浪微博。处理公开数据一般无须用户同意,平台方对第三方获取公开数据也负有一定程度的容忍义务,不适用三重授权,但第三方仍受“合理”范围内处理的限制(《个人信息保护法》第 13 条第 6 款)。“微博诉蚁坊案”判决认定平台方对公开数据仍享有合法权益,第三方应采取合法途径,若采用爬虫技术则应遵守通用技术规则。但该规则由平台方制定且通常限制白名单以外的第三方爬取,“微博诉云智联案”[②]将白名单外的第三方抓取公开数据认定为具有明显主观恶意。然而第三方往往是仰赖平台数据源的企业。因此,可借鉴美国“hiQ 实验室诉领英案”[③]适当放宽公开数据的流通范围,区分对公共利益是“好人”还是“坏人”的第三方,[④]综合判断第三方行为在竞争效能上建设性是否大于破坏性,允许对社会利益增益的第三方获取公开数据。

(三)适用场景

第三方获取其他平台数据资源主要有 4 种途径:一是通过开放应用程序接口调用平台原始数据源,即开放平台模式;二是通过爬虫技术自动爬取平台或网页数据,即爬虫模式;三是通过手机操作系统的底层设置技术获取用户在其他应用平台的数据,即手机系统模式;四是购买用户数据,即买卖个人信息。以是否获得平台授权为标准,开放平台和买卖个人信息是授权式获取,爬虫和手机系统模式是非授权式获取。

1.开放平台模式适用三重授权。《个人信息保护法》第 23 条适用于授权式获取场景,即向其他处理者“提供”。“提供”本身属于信息处理活动的一种,包括向他人传输个人数据副本或提供个人数据访问、检索途径等,应将其限缩解释为“共享”和“转让”。《信息安全技术个人信息安全规范》(GB/T35273—2020)(以下简称《安全规范》)规定,“委托处理、共享、转让、公开披露”属于对外提供,涉及两个以上的处理者。鉴于个人信息保护法另有条文明确对“委托处理”“公开”等情形提出针对性要求,通过排除法,提供则指向“共享、转让”。“共享”是处理者向其他处理者提供个人信息时“双方分别对个人信息拥有独立控制权的过程”,“转让”是将个人信息控制权由一个处理者向另一个处理者“转移的过程”(《安全规范》第 3.12 条、第 3.13 条)。开放平台模式属于“共享”,数据交换和共享的依据是“开发者协议”。尽管该协议由平台方主导,甲方色彩浓厚,但是合同主要条款效力得到司法实践普遍认可,为三重授权提供了形式正当性。“微博诉脉脉案”

① 参见北京市海淀区人民法院(2018)京 0108 民初 28643 号民事判决书、北京知识产权法院(2019)京 73 民终 3789 号民事判决书。

② 参见北京市海淀区人民法院(2017)京 0108 民初 24512 号民事判决书。

③ See hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099 (N.D. Cal. Aug. 14, 2017).

④ See Amber Zamora, Making Room for Big Data: Web Scraping and an Affirmative Right to Access Publicly Available Information Online, 12 Journal of Business, Entrepreneurship & the Law, 226 (2019).

判决认定“开发者协议”是约束开放平台合作双方的协议，双方均应本着平等互利、诚实信用、保护用户权益的基本原则合作。买卖个人信息属于“转让”，无非属于有偿提供。买卖个人信息因具有典型性而被立法从提供个人信息中独立出来加以规定。争议焦点往往围绕合同效力展开，标准为是否构成非法买卖个人信息，即未经被收集的个人同意而向他人买卖个人信息（《中华人民共和国刑法》第253条之一、《网络安全法》第44条、《民法典》第111条），如“抢楼汇诉云上城案”①“盈讯诉河南移动案”②“程某诉赵某案”③等判决均认定原、被告签订的个人信息买卖合同因未征得业主、用户、微信好友本人同意而无效。

2.爬虫模式不适用三重授权。爬虫是一种中立性技术。但第三方利用爬虫技术抓取其他平台的数据，既可能利用抓取的数据创新，也可能损害平台主机。随着数据经济价值的凸显，平台方倾向于保护自己的数据不受爬虫抓取。从法律层面看，爬虫模式不具备三重授权的形式正当性。网络服务商通过“爬虫协议”告诉第三方搜索引擎哪些页面可以抓取，哪些页面不可以抓取。不同于“开发者协议”的合同效力，爬虫协议的法律性质有“君子协议”或技术标准、行业惯例、信息服务合同中的格式条款、类似商铺“同行免进”的告示等观点。④ “奇虎诉百度案”⑤判决认定爬虫协议在本质上是一种在互联网领域内由从业者自发形成的行业惯例。从纠纷性质看，爬虫模式是依赖网络工具并利用大数据分析技术优势而获得他人控制数据的“工具型纠纷”，裁判重点不是平台授权，而是第三方是否利用不正当技术性优势进行二次开发。⑥在“微博诉饭友案”⑦中被告利用爬虫技术抓取平台内容数据并使用户不必登录微博即可直接在饭友应用程序上查看明星发布的微博，被告并未改变数据源的原初形式，对大数据技术的依赖高于“数量”因素。

3.手机系统模式不适用三重授权。第三方利用智能手机硬件终端的内置功能或手机系统自带的辅助功能绕过平台方获取用户手机上应用软件端的数据，须以“定制手机”来实现该目的。平台与第三方不具有合同、协议或技术规则等授权形式基础。第三方获取特定用户的单一数据，并不必然因“用户已同意”而具有正当性。例如，华为手机通过自带设置功能获得用户点击同意后，收集微信聊天信息并提供定向推荐服务，即使经用户同意，也要受到宪法层面通信自由和通信秘密的限制。⑧ 若第三方获取的是平台整体数据资源，涉及平台投入大量人力、物力经合法经营形成商业利益和竞争优势，则第三方的创新性竞争活动可能因影响消费者整体与长远利益提升而不具有正当性。“腾讯诉搜道案”被告通过定制手机并在其中内置群控软件突破微信产品既

① 参见广东省深圳市南山区人民法院(2016)粤0305民初3138号民事判决书。

② 参见河南省郑州市中级人民法院(2013)郑民四初字第187号民事判决书、河南省高级人民法院(2015)豫法民二终字第305号民事判决书。

③ 参见江苏省江阴市人民法院(2020)苏0281民初7297号民事判决书。

④ 参见曹阳：《我国对违反“爬虫协议”行为的法律规制研究》，《江苏社会科学》2019年第3期；许娟：《利用爬虫技术侵犯企业数据知识产权法益的司法解释》，《苏州大学学报》(哲学社会科学版)2020年第1期。

⑤ 参见北京市第一中级人民法院(2013)一中民初字第13657号民事判决书、北京市高级人民法院(2017)京民终487号民事判决书。

⑥ 参见张玉洁、胡振吉：《我国大数据法律定位的学说论争、司法立场与立法规范》，《政治与法律》2018年第10期。

⑦ 参见北京市海淀区人民法院(2017)京0108民初24510号民事判决书、北京知识产权法院(2019)京73民终2799号民事判决书。

⑧ 参见张新宝：《个人信息收集：告知同意原则适用的限制》，《比较法研究》2019年第6期。

有功能设置,新增部分功能,但因改变了微信产品既有功能被认定为非积极意义上的技术创新,对市场而言弊大于利。

三、三重授权原则的法律效果

“同意”或“授权”的使用,将影响三重授权适用的法律效果。

(一)“同意”不等于“授权”

1.“同意”与“授权”的权利基础、法律效果不同。“同意”是作出同意的一方基于意志自由,以作为或不作为的方式对提出同意请求的一方所提之请求、建议等给予肯定或否定的意思表示。① 同意为主体提供了选择可能性,是对人格尊严和意思自治的尊重。《个人信息保护法》中的“同意”包含宪法、民法等多重法律渊源,即便是民法上的“同意”也有不同的行为性质并产生不同的同意效力。“同意”是实现主体控制与选择的程序性机制,引导其从私人到公共语境的过渡,如隐私因同意公开而变为可使用的个人信息。同意的对象是特定处理行为,产生由处理者不当行为带来的事后救济效力。具体到个案,先判断特定处理行为所引发的侵权行为,后判断个人信息处理是否有其他正当理由,而个人同意是利益衡量的重要变量,即是否符合同意要求以确定是否能够阻却该处理行为的违法性。但同意并不表示信息主体放弃个人信息的主体权利,仍可在合法范围内使用该个人信息且对不当处理行为主张法律责任。即使是经过同意的处理,还须合理实施(《民法典》第 1036 条)且可随时撤回(《个人信息保护法》第 15 条),撤回的不止是同意的意思表达,实际上是撤回个人信息。“授权”是限制自己的权利为他人创设自由,或限制自己的自由为他人创设权利,意味着权利主体让渡出权利或利益的一部分。② 授权使特定行为合法化,被授权一方在授权范围内符合授权目的地自由使用。民事主体将自己的姓名、名称、肖像、声音等人格标识许可他人使用就是典型的“授权”(《民法典》第 993 条),权利基础是人格权,限制他人未经许可使用自己的姓名、肖像及其他个人特性。③ “授权”的前提是授予权利一方享有绝对支配的权利,但个人难以对其信息享有绝对、支配的控制地位,故“同意”不一定具备事先赋权的权利基础。“授权”这种范围、目的确定的许可不能随意撤回,获得授权也是被授权人行为合法的唯一基础,如果没有获得授权那么会导致侵权的法律后果,如未经权利人授权而营利性使用其肖像构成违法行为。

2.三重授权应为“用户同意+平台授权+用户同意”。“用户同意”是“我同意你做条款范围内的事”。在个人信息上存在多元利益关系,权利归属具有复合性,私权化与公共品的争论僵持不下,立法也尚未赋予个人信息绝对权地位,故用户“同意”不等于绝对权规则下的“授权”,不必然产生授权的法律效果。换言之,用户按照自主意愿和选择来决定是否允许平台或第三方处理其个人信息,不应过分解读为对个人信息的处分权利,否则易导致同意滥用而沦为处理者“保护伞”。用户同意的形式是“单独同意”,即信息主体在充分知情下单独就“向其他个人信息处理者提供其处理的个人信息”这一事项作出明确、自愿的同意。在个人信息处理中须取得单独同意的

① 参见吕耀怀:《同意的涵义、性质及其类别》,《吉首大学学报》(社会科学版)2019 年第 5 期。

② 参见高富平:《同意≠授权——个人信息处理的核心问题辨析》,《探索与争鸣》2021 年第 4 期。

③ 参见王利明:《论人格权商品化》,《法律科学》(西北政法大学学报)2013 年第 4 期。

情形都是会对个人权益产生较为重大影响的情形(《个人信息保护法》第23条、第25条、第26条、第29条、第39条)。[①] 随着处理个人信息的主体增加,个人信息数据链条延长,信息安全风险也在增加,并在一定程度上削弱信息主体和持有者的控制能力,因此下游环节要防止个人同意沦为对所有信息处理的"一次性"许可。[②] "平台授权"是平台方与第三方之间达成的合意,具备授权的形式正当性和实质正当性。形式正当性是基于"开发者协议"约定的权利义务,平台方通过技术授权来实现开放平台接口的调用权限控制与安全控制,第三方要获得相应权限才能访问平台方的数据源,"微博诉脉脉案"中脉脉因未获得高级内容权限而不能擅自获取微博平台的用户职业信息和教育信息。提供方与接收方以"合同等方式"或"约定"(《安全规范》第9.2条)来实现个人信息共享、转让时,用户非合同当事人。因此,当发现接收方违法处理个人信息时,提供方应采取一定的措施控制安全风险。当因共享、转让发生信息安全事件而对信息主体合法权益造成损害时,双方承担相应的侵权责任(《个人信息保护法》第69条)。实质正当性源于平台对共享、转让的数据享有实质性权益,因其是合法取得数据并实际控制、管理和使用用户数据的主体。

(二)三重授权的适用效力限制

1.未经三重授权不一定构成不正当竞争或个人信息侵权。三重授权体现出视同意为个人信息处理必要条件的司法审判逻辑。然而,同意并非个人信息处理唯一必要条件,未经同意也不意味着侵权。尽管同意是个人控制的实现方式,内部动因是塑造"他人眼中的自己",自由发展人格,但是却有"内在限度",这个限度就是个人利益并非总受绝对化保护,存在让位于其他合法利益的情形,[③]即其他法定合法性处理事由。在特定情况下,同意甚至并不适合作为个人信息处理的合法性事由,处理者是用户作出同意决策语境的创造者,其可以控制选择的条件,如诱导用户相信或同意。同样,司法判决通过反不正当竞争条款的适用间接确认了平台方独立的财产性利益。受"开发者协议"合同相对性的影响,是否经"平台授权"是判断第三方与平台方数据共享正当性的关键。那么是否未经平台授权就一定构成不正当竞争呢?应兼顾其他因素包括是否给竞争者带来竞争优势、平台方付出的成本、竞争对手使用数据的方式和范围等,综合判断是否违反商业道德构成直接抄袭复制数据的不劳而获行为、产品或服务直接构成实质性替代关系等后果。

2.经过三重授权并不必然具有绝对免责效力。三重授权忽视了程序意义上的同意并不一定产生实体法上的阻却违法效果,有效同意才可能阻却违法。个人同意越是不具有强迫性、同意产生的潜在风险越是容易被预测、个人越是有意识地明确同意、个人越是有持续性的可协商机会时,同意才越有效。[④] 由于一系列结构性限制和个人认知性缺陷,同意往往是不知情的、被强迫的同意及无行为能力人的同意,因此同意应仅有有限免责效力。非以同意为合法性基础时,同意便不是违法阻却事由;即使是经过同意的处理,也不绝对免责。是否达到阻却违法效果还要结合有效性、行为性质及后果等因素综合判断。

3.受正当、必要原则限制。《民法典》第1035条将"同意"与"双方的约定"并列,置于合法、正

① 参见程啸:《论个人信息处理中的个人同意》,《环球法律评论》2021年第6期。

② See Paul M. Schwartz, Property, Privacy, and Personal Data, 117 Harvard Law Review, 2056 (2004).

③ 参见于柏华:《处理个人信息行为的合法性判准——从〈民法典〉第111条的规范目的出发》,《华东政法大学学报》2020年第3期。

④ See Neil Richards, Woodrow Hartzog, The Pathologies of Digital Consent, 96 Washington University Law Review, 1465 (2019).

当、必要原则之后,体现出对同意的修正,即使同意使得处理行为合法,最小必要原则也可能使其非法。异曲同工的是欧盟“信息隐私不可让渡理论”认为数据主体不能通过同意来出售受《欧盟基本权利宪章》保护的隐私和个人数据保护基本权利,创造了“不契约”和“不同意”的区域,同意或契约的自由不能凌驾于正当、必要等基本原则之上,通过这样的设置,企业相对不容易以“同意”为其不正当处理个人信息的行为辩护。①

(三)每一重授权并非缺一不可

1.三重授权可能一重都不需要。个人同意不是处理个人信息唯一必要条件,当平台方与第三方基于同意外的其他合法性事由共享用户数据时,授权 I 和授权 III 均非必要。例如,平台方为了履行法定义务处理个人信息无须用户 A 的同意,第三方为了履行法定职责而依法强制要求平台方提供用户 A 的个人信息,第三方既无须平台授权,也无须用户 A 授权。

2.三重授权简化为“用户同意+用户同意”。用户同意是否可替代平台授权,取决于信息可携权的适用与利益衡量。信息可携权的核心是信息主体有权就其被处理的个人信息获得对应副本,以一种结构化、常用、机器可读的格式,在技术可行时,要求处理者将其个人信息直接传输给另一处理者。最初的目的是加强个人对信息的控制,但后来被视为刺激数据市场竞争和创新的监管工具。信息可携权的合理性在于其产生的外部正效应:用户对其个人信息除了有消极防御利益,还有积极利用的期待,数据的复制、下载、移转等过程都是自主决定权的组成部分,因不同用户隐私偏好不同,对个人信息积极利用的诉求不能以保护用户个人隐私或人格利益为由而否定。② 当用户行使信息可携权而同意第三方使用时,可以较好预防和打破平台经济主导下的数据垄断行为。但是鉴于平台数据类型的多样性,通过可携权实现数据共享与迁移是有适用条件的:不适用于非个人数据(单个、集合、数据产品),不适用于为公共利益或经政府授权而进行必要处理等其他合法性事由情形,不能对他人的权利及自由产生不利影响。③

3.三重授权简化为“用户同意+平台授权”。平台授权可否替代用户同意,取决于开放平台属性及个人信息在多大程度上可共享。开放平台本身具有一定的公开、公共性质,以无偿、互换和交易等方式向第三方分享用户数据,旨在拓展数据经济效益,因此既不能将平台方设置的私权技术壁垒视为当然,④也不能过多偏向用户而忽视第三方的正当使用。数据作为一项新型生产要素,只有在合理流动中才能发挥最大价值。尽管信息主体享有可携权,但是受具体市场环境及个人成本收益衡量影响,信息主体缺少足够的行权动机,以便在多个处理者之间重新分配数据价值。数量庞大的单个用户同意的成本也极高,故单纯鼓励企业自愿分享数据未必具有现实效果。因此,平台授权既是一项权利,也是平台的义务。在保护信息主体利益和平台生产者利益的前提下,平台应当分享数据,使得有正当目的的第三方可以获得数据。由于用户同意在实践中极易被架空,因此平台方负有更加严格的安全保障义务,以及对恶意第三方开发者筛选与防范的义务,

① See Paul M. Schwartz, Karl-Nikolaus Peifer, Transatlantic Data Privacy Law, 106 Georgetown Law Journal, 115 (2017).

② 参见包晓丽、熊丙万:《通讯录数据中的社会关系资本——数据要素产权配置的研究范式》,《中国法律评论》2020 年第 2 期。

③ See Helena Ursic, Unfolding the New-born Right to Data Portability: Four Gateways to Data Subject Control, 15 SCRIPTed: A Journal of Law, Technology and Society, 42 (2018).

④ 参见许娟:《互联网疑难案件中数据权利保护的风险决策树模型》,《南京社会科学》2019 年第 3 期。

平台方责任不能完全免除。

四、结　语

三重授权原则与《个人信息保护法》第23条均为“控制”格局下的界权安排。但关于控制的事实是，个人信息分析已远远超出个人的意思自治和认知范围，个人与处理者间存在严重的不对称性：个人越来越透明，处理者越来越幽暗。过于强调个人自由选择、意志和责任是一种“自负”。自负的代价是“人”被自己创造出来的“工具”掌控。因此，在强化同意规则的核心地位的同时，要弱化同意规则的功能，并延展探讨平衡个人信息保护与利用间矛盾的其他可行路径，如个人信息处理中信义义务的补充。当平台方向第三方分享其数据时，意味着未经用户直接同意的第三方也受到与平台方同等信义义务的约束。这对信息主体而言是额外保护，对个人信息处理者而言既是“限制”也是“解放”。“限制”是指须遵循信义义务的进一步限制，“解放”是指可信任的处理者将能够访问和获取更多的数据。

Abstract: The triple authorization principle is “user’s consent + platform’s authorization + user’s consent”, which is a typical description of Article 23 of the Personal Information Protection Law of the People’s Republic of China. It is a judicial rule on whether the third-party data acquisition behavior constitutes unfair competition in specific cases, and its application should be reasonably limited. On the subject, the “provider” in Article 23 can be a state organ or a non-state organ, while the “platform” in the triple authorization mode is limited to a non-state organ processor. On the object, Article 23 applies to “processed personal information”, while the triple authorization principle is limited to personal data sets and reports that the platform produces. In the scenarios, Article 23 applies to “providing personal information to other processors”, while the triple authorization principle is limited to data sharing through Open API. “Consent” and “authorization” have different legal effects. Without triple authorization does not necessarily constitute infringement, nor is it an absolute exemption by triple authorization. Each level of authorization is not indispensable.

Key Words: personal information, the triple authorization principle, unfair competition

责任编辑　　**翟中鞠**