什么是数据权利?

——从欧洲《一般数据保护条例》看数据隐私的保护

丁晓东 *

目 次

一、《条例》鸟瞰
二、《条例》述评:数据的人格权与财产权保护
三、人格权进路与隐私权进路的利弊
四、数据隐私的重新思考:消费者预期与风险规制
五、结语

摘 要 欧洲《一般数据保护条例》是全球个人数据保护的最重要立法之一。通过对该条文的分析,可以发现该法案采取了强化数据主体对个人数据控制的导向。通过对赋予给数据主体的数据隐私权的分析,可以发现这种权利同时具有人格权与财产权的特征,其边界并不清晰,也并不一定能实现立法者所期望实现的目的。保护隐私权益,应当更多采取公法风险规制与消费者法保护的框架,而不是寻求一种具有确定性边界的隐私权或个人信息权。这是因为,数据隐私必须放在特定的语境与社群中才能理解,只有结合具体语境与社群中的信息流通,才能准确思考隐私的边界与个人数据流通的合理性,才能对相关权利进行合理的界定。

关键词 《一般数据保护条例》 数据隐私 数据权利 语境 风险规制 消费者保护

2016 年 4 月 27 日,欧洲议会通过了规制个人数据或个人信息的《一般数据保护条例》(General Data Protection Regulation,英文简称 “GDPR”,下文将简称《条例》),[1] 并且已于 2018 年 5 月 25 日正式生效,替代此前的 “95 指令”。

对于这样一部极为重要的隐私与数据法,不仅欧洲国家对其进行了大量的讨论,美国等域外国家

---

* 丁晓东,中国人民大学法学院副教授,北京大学、耶鲁大学法学博士。

〔1〕 本文所使用的《一般数据保护条例》的版本为作者自己所译,参见《一般数据保护条例》,丁晓东译, http://www.sohu.com/a/232773245_455313,2017 年 10 月 5 日访问。下文引用均为此版本。

也积极参与了其立法过程,[2]而且发表了大量研究。[3]一方面,《条例》对美国商业领域和隐私法领域产生了极为重要的影响,诸如 Google、Facebook 这样的互联网企业将直接受到《条例》的管辖,一旦违反《条例》的规定,企业可能面临高额罚款。另一方面,《条例》在隐私法与数据保护领域的创新,例如被遗忘权、数据携带权等权利的规定将改写现有的隐私与数据保护法框架。如果缺少对这些问题的探讨,那么未来隐私法与数据保护法的规则制定权就将牢牢地掌握在欧洲国家的手中。

在中国,对于《条例》的介绍、讨论和参与仍然很少。目前,只有少量译介《条例》的文章与著作,而对于《条例》的全面分析,包括对《条例》所规定的被遗忘权、数据携带权、反对自动处理权的深度分析则更是处于起步阶段。[4]

这种现状无疑存在不小的问题。首先,和美国等其他国家一样,《条例》所设定的宽泛的管辖范围会对中国企业产生重大和直接影响。当中国企业数据业务涉及"为欧盟内的数据主体提供商品或服务——不论是否要求数据主体进行支付",或者"监控发生在欧洲范围内的数据主体的活动"时,[5]就受到《条例》的规制。这就是说,如果某家中国企业通过相关数据分析欧盟某成员国的消费者数据以准备供货订单,或者分析中国公民在欧盟内活动的数据,即使他们使用的是诸如微信、淘宝这样的平台,也必须遵守《条例》的规则。[6]其次,从未来隐私法与数据保护的规则制定来说,对于《条例》的整体分析以及对其具体制度的深度分析也具有迫在眉睫的需求。尽管中国的互联网企业和其他企业已经具备了和美国等大型企业竞争的能力,但在隐私与数据保护规则等方面,中国的企业与知识界的准备却远远不足。可以想见,如果未来中国企业希望进入欧洲市场,或者进入其他隐私与数据保护标准较高的市场,其所面临的制度风险将远远超过欧洲企业和美国企业。最后,从学术的层面来看,《条例》所规定的一系列数据主体的权利已经对现有的法律理论提出了新的挑战。如何理解隐私与个人数据?个人数据是一种个人可以随意处置的财产或准财产,还是不可以随意处置的个人人格的一部分?对隐私与个人数据的保护应当采取财产权保护的框架,还是人格权保护的框架?或者是否应当将个人数据视为一种知识产权,采取知识产权的保护框架?对《条例》进行分析,将有助于我们理解这些根本性的学术问题。

基于这些考虑,本文将首先介绍《条例》的整体框架与重点条文,指出《条例》从整体上采取了一种强化数据主体权利的进路。随后指出这种强化数据主体权利的进路面临着界定的难题:无论是将数据隐私界定为一种人格权还是界定为一种财产权,都面临着不小的困境。究其原因,现有对数据权利、隐私权、人格权与财产权的思考都没有充分考虑语境与社群的隐私。一旦我们将这些概念与特定语境与社群中的信息流通结合起来,就能更合理地理解数据隐私的本质,也能够更好地反思数据隐私保护的法律框架。保护数据隐私不应当期待可以寻求某种客观的权利边界,而应当更多采取风险规制的公法框架与尊重预期的消费者法框架,通过这两个框架来界定相关权利的边界。

---

〔2〕 Kevin Collier, "U.S. Lobbyists Are Writing Europe's Data Protection Rules, Daily Dot" (Feb. 11, 2013, 14:25 CT), http://www.dailydot.com/news/us-lobbyists-european-data-privacy/, accessed October 5, 2017.

〔3〕 在美国法学院的法律评论杂志上,已经有数百篇对《条例》进行研究的论文。

〔4〕 本文的写作始于 2016 年底,在本文写作之际,对《条例》的翻译与评论仍然较少。在本文付梓之际,对《条例》的翻译与分析已经增加很多。相关的研究,可参见高富平:《个人数据保护和利用国际规则:源流与趋势》,法律出版社 2016 年版;京东法律研究院:《欧盟数据宪章:〈一般数据保护条例〉(GDPR)评述及实务指引》,法律出版社 2018 年版。

〔5〕 见《条例》第 3 条第 2 段。

〔6〕 当然这是对《条例》的字面解读,《条例》的管辖范围到底有多宽,这仍有待于欧盟的执法实践来进行确定。而这里提到的两种情形,前一种情形受到《条例》管辖的可能性要大得多。

一、《条例》鸟瞰

从章节设置来看,《条例》一共分为十一章,分别是一般条款;原则;数据主体的权利;控制者和处理者;将个人数据转移到第三国或国际组织;独立监管机构;合作与融贯性;救济、责任与惩罚;和特定处理情形相关的条款;授权法案与实施性法案;最后条款。

第一章规定了《条例》所涉及的主要事项与目标、适用范围、地域管辖范围以及相关概念的定义。就主要事项与目标来说,《条例》开宗明义,"本条例制定关于处理个人数据中对自然人进行保护的规则,以及个人数据自由流动的规则",[7]将保护自然人的自然数据权利和设定个人数据自由流动规则作为条例的主要事项与目标。就适用范围来说,条例设定了宽泛的管辖权,[8]例如,就地域管辖范围来说,条例除了规定在欧盟内部设立的数据控制者或处理者的数据处理受本条例管辖之外,[9]还规定了"为欧盟内的数据主体提供商品或服务——不论是否要求数据主体进行支付;或者监控发生在欧洲范围内的数据主体的活动",此类数据处理也受条例的管辖。这就意味着,如果《条例》得到严格执行,《条例》的管辖范围不仅仅限于欧盟内部,而且会影响到其他各国企业与实体的数据处理。就定义来说,其中最为重要的是个人数据的定义:"'个人数据'的含义是任何已识别或可识别的自然人('数据主体')相关的信息;一个可识别的自然人是一个能够被直接或间接识别的个体,特别是通过诸如姓名、身份编号、地址数据、网上标识或者自然人所特有的一项或多项的身体性、生理性、遗传性、精神性、经济性、文化性或社会性身份而识别个体。"[10]

第二章是数据处理的一般原则。《条例》规定了六项原则。[11](a)"合法性、合理性和透明性"原则:"对涉及数据主体的个人数据,应当以合法的、公平的和透明的方式来进行处理。"(b)"目的限制"原则:"个人数据的收集应当遵循具体的、清晰的和正当的目的,对个人数据的处理不应当和此类目的不相容。"(c)"数据最小化"原则:个人数据对于为了实现数据处理目的应当是适当的、相关的和必要的。(d)"准确性"原则:个人数据应当是准确的,如有必要,必须及时更新;必须采取所有步骤,保证为了实现某项目的而处理的不准确的个人数据被擦除或及时更正。(e)"限期储存"原则:"对于能够识别数据主体的个人数据,其保存方式应当不长于为了实现个人数据处理目的所必要的期限;超过此期限的数据处理只有在如下情况下才能被允许:为了实现公共利益、科学或历史研究目的或统计目的,为了保障数据主体的权利和自由,并采取了本条例第89(1)条所规定的合理技术与组织措施。"(f)"诚实与保密"原则:"个人数据的处理应当通过合理的技术或组织手段,保障个人数据的合理安全,包括防御未授权或非法的处理,防御意外损失、销毁或损害。"同时,《条例》还规定"可问责性"原则,控制者除了遵守以上五点处理原则,"而且应当有责任对此提供证明"。[12]

第二章还对处理的合法性所需满足的条件作出了规定。第6条规定,处理的合法性必须满足某项条件,例如"数据主体已经同意基于一项或多项目的而对其个人数据进行处理"。而在数据主体未

〔7〕 第1条第1段。

〔8〕 第2条第1段规定:除了某些情形,"本条例适用于对个人数据进行全部或部分性的个人数据处理"。

〔9〕 第3条第1段。

〔10〕《条例》还对处理、控制者与处理者等概念进行了定义。见《条例》第4条第(2)项、第(7)项、第(8)项。

〔11〕 第5条第1段(a)(b)(c)(d)(e)(f)。

〔12〕 第5条第2段。

表示同意的情形下,处理的合法性必须是为了实现数据主体利益、[13]履行公共职责、[14]保护第三人核心利益、[15]实现公共利益、[16]控制者或第三人的正当利益[17]。而对于何谓数据主体的同意,《条例》做出了标准很高的规定。控制者首先负有举证责任,其有责任证明“数据主体已经同意对其个人数据进行处理”。[18]其次,“如果数据主体的同意是在涉及其他事项的书面声明的情形下作出的,请求获得同意应当完全区别于其他事项,并且应当以一种容易理解的形式,使用清晰和平白的语言”,任何控制者所发表的免责声明都不具有效力。[19]再次,“数据主体应当有权随时撤回其同意”。[20]最后,《条例》还规定,“分析同意是否是自由做出的,应当最大限度地考虑的一点是:对契约的履行——包括履行条款所规定的服务——是否要求同意履行契约所不必要的个人数据处理。”[21]

第三章规定了数据主体所拥有的权利。第 12 条至第 14 条规定数据主体获取信息的权利,在收集数据主体信息之前,其有权获取控制者的身份与详细联系方式、处理目的等相关信息。第 15 条至第 22 条规定了数据主体对个人数据的访问权、更正权、擦除权(“被遗忘权”)、限制处理权、数据携带权、一般反对权和反对自动化处理的权利。其中,最重要的当属对数据的访问权、更正权、擦除权与携带权。

就访问权而言,《条例》规定“数据主体应当有权从控制者处得知,关于其个人数据是否正在被处理”,而如果正在被处理的话,数据主体“有权访问个人数据”和获知一系列信息,包括处理的目的、相关个人数据的类型、个人数据已经被或将被披露给接收者或接收者的类型、个人数据将被储存的预期期限、数据主体所拥有的相关权利。[22]就更正权而言,《条例》规定:“数据主体应当有权从控制者那里及时得知对与其相关的不正确信息的更正。在考虑处理目的的前提下,数据主体应当有权完善不充分的个人数据,包括通过提供额外声明的方式来进行完善。”[23]就擦除权(“被遗忘权”)而言,《条例》规定在某些情形下,“数据主体有权要求控制者擦除关于其个人数据的权利”。例如,如果“个人数据对于实现其被收集或处理的相关目的不再必要”,[24]或者数据主体撤回同意,[25]或者“已经存在非法的个人数据处理”。[26]就携带权而言,《条例》规定:“数据主体有权获得其提供给控制者的相关个人数据,而且其获得个人数据应当是经过整理的、普遍使用的和机器可读的,数据主体有权无障碍地将此类数据从其提供给的控制者那里传输给另一个控制者。”[27]

---

〔13〕 参见第 6 条第 1 段第(b)项:“处理对于完成某项数据主体是一方的契约是必要的,或者在签订契约前为了完成数据主体的请求而进行的处理。”

〔14〕 参见第 6 条第 1 段第(c)项:“控制者是某项法律职责的主体,而处理对于履行此项法律职责是必要的。”

〔15〕 参见第 6 条第 1 段第(d)项:“处理是为了保护数据主体或另一个自然人的核心利益所必要的。”

〔16〕 参见第 6 条第 1 段第(e)项:“数据控制者为了公共利益或基于官方权威而履行某项任务而进行的处理。”

〔17〕 参见第 6 条第 1 段第(f)项:“处理对于控制者或第三方所追求的正当利益是必要的。”

〔18〕 第 7 条第 1 段。

〔19〕 第 7 条第 2 段。

〔20〕 第 7 条第 3 段。

〔21〕 第 7 条第 4 段。

〔22〕 第 15 条第 1 段。

〔23〕 第 16 条。

〔24〕 第 17 条第 1 段第(a)项。

〔25〕 参见第 17 条第 1 段第(b)项:“处理是根据第 6(1)条(a)点,或者第 9(2)条(a)点而进行的,而且没有处理的其他法律根据,数据主体撤回在此类处理中的同意。”

〔26〕 第 17 条第 1 段第(d)项。

〔27〕 第 20 条第 1 段。

第四章规定了数据控制者和处理者的责任。其中第一部分第25条至第31条规定了控制者与处理者的一般责任。例如第25条规定,控制者必须承担"通过设计的数据保护和默认的数据保护(data protection by design and by default)"的责任。所谓通过设计的数据保护,指的是控制者应当有一套固有的数据保护机制,而不只是采取一些临时性和个案性的保护措施。[28]而所谓的默认的数据保护,指的是控制者的数据保护责任是一种缺省规则。[29]第二部分规定了控制者与处理者对于个人数据安全所应承担的责任和采取的措施。例如第32条规定,在考虑了"最新水平、实施成本、处理的性质、处理的范围、处理的语境与目的之后,以及处理给自然人权利与自由带来的伤害可能性与严重性之后",控制者和处理者应当采取"适当技术与组织措施,以便保证和风险相称的安全水平"。第三部分规定了数据保护影响评估与数据处理之前的事先咨询要求。例如第35条规定,当数据处理对个人因素"进行系统性与全面性的评价"并且"其决策对自然人产生法律影响或类似重大影响"时,[30]处理特定类型的数据或犯罪相关数据时,[31]或者数据处理与大规模的方式系统性地监控某个公众可以访问的空间相关时,[32]"控制者应当在处理之前评估计划的处理进程对个人数据保护的影响"。[33]第四部分是关于数据保护官的规定。例如第37条规定,在某些情形下,如在公共机构的数据处理、大规模数据处理或者特殊数据处理中,控制者和处理者应当委任数据保护官。[34]数据保护官具有"对控制者或处理者,以及那些履行本条例和欧盟其他成员国数据保护条款所规定的处理责任的雇员进行告知,提供建议"、确保控制者和处理者遵守条例、和监管机构合作等职责。[35]同时,数据保护官应当保持其自身的独立性。第五部分规定的是行业协会等实体所自行起草的数据保护的行为准则与欧盟内部的认证机制。例如第42条规定了认证机制,"成员国、监管机构、欧盟数据保护委员会和欧盟委员会应当鼓励——尤其是在欧盟层面——建立数据保护认证机制、数据保护印章和标记,以证明控制者和处理者的处理操作符合本条例"。[36]《条例》还规定,参与认证应当是自愿的,[37]而且认证应当由有权监管机构等有资质的实体所授予[38]。

第五章是关于将个人数据转移到第三国或国际组织的规定。第44条首先规定了此类转移的一般原则:"对于正在处理或计划进行处理的个人数据,将其转移到第三国或国际组织,包括将个人数据从第三国或国际组织转移到另一第三国或另一国际组织,控制者和处理者只有满足本条例的其他条

〔28〕 参见第25条第1段:"在考虑了最新水平、实施成本、处理的性质、处理的范围、处理的语境与目的,以及处理给自然人权利与自由带来的伤害可能性与严重性之后,控制者应当在决定处理方式时和决定处理时应当采取合适的技术与组织措施,并且在处理中整合必要的保障措施,以便符合本条例的要求和保护数据主体的权利。例如,控制者可以采取匿名化,一种设计用来实施数据保护原则——比如数据最小化原则——的措施。"

〔29〕 参见第25条第2段:"控制者有责任采取适当的技术与组织措施,以保障在默认情况下,只有某个特定处理目的所必要的个人数据被处理。这种责任适用于收集的个人数据的数量、处理的限度,储存的期限以及可访问性。尤其需要注意的是,此类措施必须确保,在默认情况下,如果没有个体介入,个人数据不能为不特定数量的自然人所访问。"

〔30〕 第35条第1段(a)。

〔31〕 第35条第1段(b)。

〔32〕 第35条第1段(c)。

〔33〕 第35条第1段。

〔34〕 第37条第1段。

〔35〕 第39条。

〔36〕 第42条第1段。

〔37〕 第42条第3段。

〔38〕 第43条第1段。

款,以及满足本章规定的条件才能进行转移。为了保证本条例对于自然人的保护程度不会被削弱,本章的所有条款都应当被遵守。”[39]其次,规定了两种类型的转移,第一种是“基于充分性的转移”,当欧盟委员会作出决定,“认为相关的第三国、第三国中的某领地或一个或多个特定部门、或国际组织具有充分性的保护,可以将个人数据转移到第三国或国际组织。此类转移不需要特定的授权。”[40]另一种情况则是不具备充分性的转移,当欧盟委员会认为第三国、第三国内的领地或一个或多个特定部门、或国际组织不具有充分程度的保护,“控制者或处理者只有提供适当的保障措施,以及为数据主体提供可执行的权利与有效的法律救济措施,才能将个人数据转移到第三国或一个国际组织”。[41]

第六章是关于独立监管机构的规定。关于其设立,第 51 条规定,“每个成员国应当建立一个或多个独立公共机构,负责监控本条例的实施”。[42]关于其权力,每个监管机构都具有调查权力:例如,要求控制者和处理者提供履行其任务所需要的所有信息;以数据保护核查的方式进行调查;对认证进行审查;将可能侵犯本条例的情况告知控制者或处理者;从控制者或处理者那里获取访问个人数据的权力;获取对控制者和处理者的所有房屋建筑及场地,包括数据处理设施和方法的访问权等等。[43]在此章中,还对欧盟数据委员会的设立、目标和责任等进行了规定。[44]

第七章是关于合作与一致性的规定。由于每个成员国都具有一个或多个独立监管机构,欧洲各成员国在监管问题上需要相互配合、相互协作,采取多方面措施确保对《条例》的适用具有一致性。例如,对于具有领导性监管机构的情形,第 60 条要求“领导性监管机构应当根据本条和其他相关监管机构进行合作,努力达成共识。领导性监管机构和相关监管机构应当彼此分享相关信息”。[45]

第八章是关于救济、责任与惩罚的规定。在这一章中,除了规定每个数据主体“向监管机构提起申诉的权利”,[46]“针对监管机构的有效司法救济的权利”,[47]“针对控制者或处理者的有效司法救济权”,[48]还对违反《条例》所应承担的行政罚款做了规定。如果违反《条例》的某些非核心条款,可以“施加最高 10 000 000 欧元的行政罚款”或“前一年全球总营业额 2% 的罚款”(两者取其高);[49]而如果违反《条例》所规定的某些核心条款,例如,处理的基本原则、同意的条件、数据主体的权利、将个人数据转移到第三国或一个国际组织的接收者,则可以“施加最高 20 000 000 欧元的行政罚款”或“前一年全球总营业额 4% 的罚款”(两者取其高)。[50]

第九章是与特定处理情形相关的条款。其中较为重要的是第 85 条,该条规定:“成员国应当通过制定法律调和符合本条例制定的个人数据保护权与表达自由权与信息权,包括调和为了新闻目的和学术、艺术或文学表达目的而进行的处理。”同时,对于“为了新闻目的和学术、艺术或文学表达目的

〔39〕 第 44 条第 1 段。
〔40〕 第 45 条第 1 段。
〔41〕 第 46 条。
〔42〕 第 51 条第 1 段。
〔43〕 第 58 条第 1 段。
〔44〕 第 68 条第 1、3 段。
〔45〕 第 60 条第 1 段。
〔46〕 第 78 条。
〔47〕 第 79 条。
〔48〕 第 80 条。
〔49〕 第 83 条第 4 段。
〔50〕 第 83 条第 5 段。

而进行的处理,如果对于调和符合本条例制定的个人数据保护权与表达自由权与信息权有必要,成员国应当对第二章(原则)、第三章(数据主体的权利)、第四章(控制者和处理者)、第五章(个人数据转移到第三国或国际组织)、第六章(独立监管机构)、第七章(合作与一致性)和第九章(特定数据处理的情形)的规定进行豁免或克减"。

第十章"授权法案与实施性法案"与第十一章"最后条款"是关于《条例》细化的权力与《条例》的解释问题。第92条规定,"制定授权法案的权力被授权给欧盟委员会,此权力受本条所规定的条件所约束"。[51]《条例》最后规定:"本条例的所有条款都具有约束力,而且应当直接适用于成员国。"[52]

二、《条例》述评:数据的人格权与财产权保护

《条例》涉及个人数据保护的方方面面,但综合来看,仍然可以发现其中有一条非常明显的主线,就是强化数据主体对于数据的控制权。如同《条例》所规定的,"本条例保护自然人的基本权利与自由,特别是保护自然人享有的个人数据保护的权利。"[53]或者如欧盟委员会前副主席芮丁女士(Viviane Reding)所言,"个人数据保护对于欧洲人而言是一项基本权利",欧洲一直将"隐私视为一种建立在基本人权之上的政治要求"。[54]

《条例》的很多条文都体现了这一特征。首先,《条例》将同意作为处理的基本原则,对于个人数据的收集、储存、处理、披露都必须获取个人的同意。而缺乏同意的处理只有在例外情形下,如为了实现数据主体利益、履行公共职责、保护第三人核心利益、实现公共利益、控制者或第三人的正当利益才能进行处理。[55]其次,即使在获取了数据主体的同意后,数据主体也仍然拥有多项对于数据的权利,数据主体仍然拥有对于数据的访问权、更正权、擦除权("被遗忘权")、限制处理权、数据携带权、一般反对权和反对仅仅基于自动化的个人决策的权利。对于这些权利,《条例》规定数据控制者或处理者不得要求数据主体放弃这些权利以换取服务。最后,《条例》详细规定了数据主体向独立监管机构以及司法机构提起诉讼的权利,可以要求数据控制者或处理者遵守数据主体的权利,并且在数据控制者或处理者违反数据主体权利时进行赔偿。

对于条例的这些规定,我们应当思考的是,《条例》所规定和强化的数据主体的权利是一种什么性质的权利?当《条例》对某项权利没有进行明确规定,或者当人们对于《条例》的某种权利存在争议时,应当以何种权利属性来进行分析和解释?有人或许会说,《条例》所规定的数据主体的权利是一种隐私权,因为一般认为,《条例》以及更早的"95指令"所涉及的问题都是隐私问题的分支:信息隐私或数据隐私。但对于这一回答,仍然不可避免地会面临进一步的追问:什么是隐私权?隐私权或者说《条例》所规定的数据主体的权利是人格权吗?抑或是一种财产权?甚至可能是一种知识产权?对于这些问题,我们有必要一一做出分析,这不仅仅是一个理论问题,而且也将是关乎到如何解释《条

〔51〕 第92条第1段。

〔52〕《条例》最后一段。

〔53〕 第1条第2段。

〔54〕 Q. and A. with Viviane Reding, N.Y. Times, Feb. 2, 2013, http://www.nytimes.com/2013/02./03/business/q-and-a-with-viviane-reding.html,accessed October5, 2017. See generally Joel R. Reidenberg, "E-Commerce and Trans-Atlantic Privacy" 38 *Hous. L. Rev.* 717, 730-32(2001).

〔55〕《条例》将个人规定为数据主体,将企业与公司等规定为数据控制者或处理者,也表明了这一点。

例》与适用《条例》、如何设置个人数据保护规则的实践性问题。

（一）数据隐私的人格权保护

我们可以首先分析人格权保护的进路。早在 1890 年，在沃伦（Smauel Warren）与布兰代斯（Louis Brandeis）所发表的经典文献《隐私权》中，[56] 沃伦与布兰代斯就提出了一种基于不可侵犯的人格权的隐私权，在他们看来，随着大众媒体的兴起与私人空间日益被各种媒体所侵犯，有必要发展出一种普通法上的“一般隐私权利”，普通法应当保护“思想、情绪和感受（thoughts, emotions, and sensations）”这些构成人格的要素。[57] 其后，虽然美国法在实践中日渐抛弃了以人格权来理解隐私权的进路，[58] 但仍然有美国学者坚持应当以人格权来分析隐私权。[59] 而在德国，基于人格权的隐私保护则成为了主流进路。德国联邦最高法院先后通过“读者来信案”（Schacht judgment of 1954）、[60] 1958 年的“骑士案”、[61] 1973 年的伊朗王后案（Soraya）案 [62] 确立了对个人隐私的人格权保护。

从《条例》的规定来看，某些条款的确显示了《条例》对数据隐私的人格权保护。例如，《条例》第 9 条规定，“对于那些显示种族或民族背景、政治观念、宗教或哲学信仰或工会成员的个人数据、基因数据、为了特定识别自然人的计量生物学数据、以及和自然人健康、个人性生活或性取向相关的数据，应当禁止处理”。[63] 第 22 条第 1 段规定，“数据主体应当有权不被仅仅靠自动化处理——包括归档——来对其做出对数据主体产生法律影响或类似严重影响的决策”。[64] 这些规定表明，《条例》认为应当禁止涉及个人人格的数据，而且，数据主体应当是具有主体性的个人，用康德的术语来说，就是人必须成为目的而不是手段，对个人具有法律影响或重大影响的决策，不能仅仅通过自动化处理来作出。

但另一方面，很难说《条例》整体上采取了人格权保护的进路。如上所述，《条例》最大的特征在于强化数据主体的权利或对于个人数据的控制，即使数据控制者或处理者对于个人数据的处理不会影响到个人的人格，数据主体也有权利拒绝数据控制者的收集，以及拥有对于数据的访问权、更正权、擦除权（“被遗忘权”）、限制处理权、数据携带权等权利。

（二）数据隐私的财产权保护

在某种程度上，《条例》强化个人数据控制权的进路继承了著名的隐私法学者阿兰 • 威斯丁（Alan Westin）的隐私观。1967 年，威斯丁出版了现代隐私法上里程碑式的著作《隐私与自由》。在这本书里，

---

〔56〕 Samuel D. Warren & Louis D. Brandeis, “The Right to Privacy” 4 *Harv. L. Rev*. 193（1890）.

〔57〕 Samuel D. Warren & Louis D. Brandeis, “The Right to Privacy” 4 *Harv. L. Rev*. 193, 195, 206（1890）.

〔58〕 美国隐私法受到美国学者威廉姆 • 普罗斯（William Prosser）的巨大影响，对此的分析，参见 Neil M. Richards & Daniel J. Solove, “Prosser’s Privacy Law: A Mixed Legacy” 98 *Calif. L. Rev.* 1887（2010）.

〔59〕 Edward J. Bloustein, “Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser” 39 *N.Y.U. L. Rev*. 962（1964）.

〔60〕 在此案中，德国联邦最高法院认为《德国基本法》第 1 条第 2 款所提到的个人尊严可以作为德国民法上的渊源性权利，这样，个体作为“人的尊严和发展其个体人格”的利益应当受到民法的保护，这一人格权应当可以对抗不特定的第三人。对于此案的介绍，参见［德］迪特尔 • 梅迪库斯：《德国民法总论》，邵建东译，法律出版社 2013 年版，第 805-807 页。

〔61〕 在此案中，德国联邦最高法院在“骑士案”中确认了对伤害人格权行为的损害赔偿，认为对人格权的伤害具有和一般性的人身伤害同等严重。

〔62〕 在此案中，德国联邦最高法院认为，《德国基本法》第 1 条和第 2 条保护了“个人的隐私领域”；个人有权“行使独处的愿望”，保持“自身不被外界打扰”。Federal Constitutional Court, BVerfGE 34, 269, 281, 转引自 Paul M. Schwartz & Karl-Nikolaus Peifer, “Prosser’s Privacy and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept?” 98 *Cal. L. Rev*. 1925（2010）.

〔63〕 第 9 条。

〔64〕 第 22 条第 1 段。

威斯丁认为,隐私的关键是对信息的控制,即“个人、群体或机构对自身信息在何时、如何以及在何种程度上与他人沟通的主张”。[65] 其后,威斯丁又于 1972 年出版了《自由社会中的数据库》,详述了当代的计算机框架如何制造了新的隐私的问题,并且提出类似的个人对于信息与数据的控制权。[66]

对于这种强化个人数据控制权的隐私的进路,不少学者发展出了个人数据财产权的观念。例如,保罗·施瓦茨(Paul Schwartz)教授、维拉·柏格森(Vera Bergelson)教授、爱德华·简格(Edward J. Janger)都指出,在现行法律下,法律没有提供诸如强制令(injunction)之类的事前救济,也没有提供惩罚性赔偿的保护手段。他们借用卡拉布雷西在其名作《大教堂一瞥:财产规则、责任规则与不可让渡性》中所提到的责任规则与财产规则的区别,[67] 认为当前的法律,无论是美国还是欧洲,只对隐私提供了基于责任规则的保护,而没有提供基于财产规则的保护,未来有必要以财产规则来对隐私进行保护。[68] 而莱西格教授(Lawrence Lessig)也曾经在其网络法名著《代码》中提出过个人数据财产权的观点,他认为,赋予个人数据以财产权,这有利于提高个人在和公司等实体机构中的谈判权,更好地保护个人利益。[69]

而对于《条例》,有的评论者认为,其对于数据隐私恰巧采取了财产权或准财产权的保护。例如,在《耶鲁法律评论》的一篇评论文章中,雅各布·维克托(Jacob M. Victor)指出,《条例》虽然没有明确确立个人数据的财产权保护,但其对个人数据的规定有三个特征,这些特征都表明《条例》将个人数据视为一种财产。其一,《条例》确立了默认权利(default entitlements)的原则,收集与处理个人数据不仅需要征得个人同意,而且在没有明确个人同意的情况下,个人也是其数据的默认拥有者。其二,《条例》为数据本身设定了某些责任,即使他人通过合同或数据主体的同意而获得了数据,他们也必须对这些数据承担某些义务,而不能随意处分这些数据。其三,《条例》规定了基于财产规则的救济(property-rule-based remedies)。条例规定,合法的数据收集与处理只能是基于个人同意的,在没有个人同意的情形下,个人可以进行申诉、提起司法诉讼,而监管机构也可以对数据控制者与处理者施加高额处罚。[70]

在一定程度上,这种以数据财产权来理解《条例》的观点具有很强的说服力。的确,维克托所归纳的三个特征都具有财产权的特征。《条例》设置了数据主体对于其个人数据的默认权利,这说明了条例强化个人对其数据进行控制的立场,对于个人数据施加了一种类似知识产权的保护。[71]《条例》为数据本身设定了责任,要求数据的控制者或处理者不能随意处置数据,这说明了数据主体的利益已

---

〔65〕 Alan Westin, *Privacy and Freedom*, Atheneum, 1967, p. 7.

〔66〕 Alan Westin & Michael A. Baker, *Databanks in a Free Society*, Quadrangle Books, Inc., 1972.

〔67〕 Guido Calabresi & A. Douglas Melamed, “Property Rules, Liability Rules, and Inalienability: One View of the Cathedral” 85 *Harv. L. Rev*. 1089 (1972).

〔68〕 Paul M. Schwartz, “Property, Privacy, and Personal Data” 117 *Harv. L. Rev*. 2055 (2004); Edward J. Janger, “Privacy Property, Information Costs, and the Anticommons” 54 *Hastings L.J.* 899 (2003); Vera Bergelson, “It’s Personal but Is It Mine? Toward Property Rights in Personal Information” 37 *U.C. Davis L. Rev*. 379 (2003).

〔69〕 Lawrence Lessig, *Code and Other Laws of Cyberspace*, Basic Books, 1999, pp. 122-35, pp. 159-63; 也可参见 Lawrence Lessig, “The Architecture of Privacy” 1 *Vand. J. Ent. L. & Prac.* 56, 63-64 (1999); Lawrence Lessig, “Privacy as Property” 69 *Soc. Res*. 247, 261 (2002).

〔70〕 Jacob M. Victor, “The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy” 123 *Yale L.J.* 513(2013).

〔71〕 对于以知识产权来保护隐私与个人数据的讨论,参见 Pamela Samuelson, “Privacy as Intellectual Property” 52 *Stan. L. Rev.* 1125(2000).

经被“内置于(built-in)”数据中。[72]《条例》所设置的救济方式也表明,《条例》对于个人数据的保护是基于财产规则而不是责任规则,对于违反个人同意而进行的数据收集与处理,《条例》所规定的赔偿是惩罚性的而不是补偿性的。

但另一方面,《条例》却在自由处分与自由交易这一点上与传统的财产权理论相去甚远。对于传统的财产权理论来说,个人基于其意志而自由处分其财产,包括出售其财产,这是财产权的重要特征。而一旦个人基于其意志而出售财产,获得财产的一方应该也能获得对财产的所有权与处置权。而《条例》却没有赋予数据主体以完全自由交易的权利和赋予企业等实体以数据所有者的权利。在很多规定上,《条例》仍然采取了基本权利的进路,赋予数据以某些不可转让的特征。例如,虽然《条例》规定的数据主体的权利和知识产权具有一定的相似性,但这种权利却更类似于法国语境下的建立在人格权进路上的知识产权保护。在法国的知识产权框架中,个人永远无法完全出售其知识产权,即使艺术家出售了其作品,购买者也不能对其作品进行恶意修改或损毁。[73]同样,在《条例》的框架下,即使个人同意,数据控制者和处理者也不能完全获得对其数据的控制权与处理权,数据控制者与处理者对个人数据的收集、储存、处理与披露仍然必须遵守《条例》所赋予给数据主体的某些权利。

在这个意义上,《条例》对于个人数据的保护并没有完全采取一种财产法的进路,仍然保留了很强的人格权保护的色彩。如同财产法研究学者玛格丽特·简·拉丁(Margaret Jane Radin)指出的,计算机世界对于信息隐私或数据隐私的财产化或商品化是不完全的。在她看来,“将隐私视为一种与个人人格相关的人权,还是视为一种为个人所拥有和控制的财产,这具有本质性的不同……人权一般被假定为不可以在市场上交易,而财产则一般被假定为可以在市场上交易”。[74]

三、人格权进路与隐私权进路的利弊

如何评价《条例》对于数据隐私兼顾人格权与财产权的保护?在此,我们可以首先分析这两种进路的利弊,以此来进一步反思《条例》对于数据隐私的规定。

(一)人格权进路的利弊

对于数据隐私的人格权保护来说,其优点在于人格权是一种较为抽象性的权利,可以为数据主体提供一种发展中的权利或较为宽泛的保护。例如,擦除权或被遗忘权可能很难在财产权的框架中得到保护,因为在财产权的框架中,一旦财产进行合法转移,其所有权和处分权就应当在购买者手中,出售人无权要求购买者进行销毁或“遗忘”。但在人格权的理论体系中,则可以论证,计算机与网络等现代技术已经完全改变了历史上的信息记录机制,[75]当计算机与网络的信息记录机制对某些人的人格造成了损伤,个体应当有权要求数据控制者擦除其个人数据。[76]

---

〔72〕 Paul M. Schwartz, “Property, Privacy, and Personal Data” 117 *Harv. L. Rev*. 2055, 2098 (2004).

〔73〕 Henry Hansmann & Reinier Kraakman, “Property, Contract, and Verification: The Numerus Clausus Problem and the Divisibility of Rights” 31 *J. Legal Stud*. S373, S368-387 (2002).

〔74〕 Margaret Jane Radin, “Incomplete Commodification in the Computerized World”, in Niva Elkin-Koren & Neil Weinstock Netanel ed., *The Commodification of Information*, Hague: Kluwer Law International, 2002, p. 17.

〔75〕 对互联网记忆机制的一个分析,参见 Demi Marks, “The Internet Doesn’t Forget: Redefining Privacy through an American Right to be Forgotten” 23 *UCLA Ent. L. Rev*. 41(2016).

〔76〕 对于本文而言,这里重要的不在于擦除权或被遗忘权是否完全正当,而在于被遗忘权或擦除权提供了一个范例,可以对个人隐私提供更为宽泛的保护和发展中的保护。

但另一方面,人格权的优点也可以说恰巧是其缺点。人格权或许能为数据主体提供较为宽泛的保护,而且能够适应时代而不断发展出新的权利类型,但对于企业和其他实体来说,这就意味着他们必须不断提供新的保护责任,并为此承担并不轻松的人力与资金负担。例如,在欧洲树立被遗忘权或擦除权之后的一年多内,谷歌等公司就收到了数十万的请求,要求对一百多万条网页信息进行删除。[77]而在收到这些请求后,谷歌公司又不可以以自动化的方式对所有这些信息进行一键删除。为了保证公众的知情权和其他权利,谷歌公司必须采取个案式的审查,区分具有正当性基础和不具有正当性基础的信息删除。这为谷歌公司增加了不小的负担。

携带权则是另一个会给企业等实体增加负担的例子。《条例》首次提出了数据主体对个人数据的携带权利,规定"数据主体有权无障碍(without hindrance)地将此类数据从其提供给的控制者那里传输给给另一个控制者"。[78]这意味着在数据主体的请求下,数据控制者必须能够将个人数据打包供个人下载,甚至转移到第三方的网站或实体。相比擦除个人数据,这对网络公司与其他数据控制公司提出了更高的技术要求,因为不同公司或实体之间的网站可能无法实现数据直接传输,如果要真正落实"无障碍"传输,网站可能需要具备某种软件代码或所谓的"输出—输入组件"(export-import module)。对于刚起步的互联网企业来说,这意味着他们的成本将随之提高。[79]

除此之外,人格权的开放性与模糊性也存在某些问题。人格权的开放性与模糊性可以为数据主体提供更多的权利保护,但也可能会导致权利边界的不确定性。尽管人们可能会对基于同意和财产权的商品化交易做出种种批评,例如,网站的隐私条款往往晦涩难懂、[80]数据主体的同意可能不是基于真实的意思表示,[81]但同意的好处在于其提供了一种简单、明确的交易规则,使得双方能够在数据收集阶段就对数据的归属或处理方式达成合意。[82]相反,以人格权的方式来对数据隐私进行保护,则用户的同意可能会面临形同虚设的局面,企业或互联网公司将很难把握其处理是否是合法的,是否侵犯了个人人格尊严。

(二)财产权进路的利弊

在某种程度上,数据隐私财产权保护进路的利弊恰好与人格权保护的进路相反。如上所述,如果说人格权的进路具有开放性与模糊性,会造成规则的不明确性,那么基于传统财产权的交易规则则较为明确,这种规则将个人同意至于数据流通的核心,认为个人是对其自身数据的最佳判断者。同时,如果说人格权的开放性与模糊性可能会给企业带来较大的负担,从而不利于小微企业的创新,那么基于同意与财产权的交易规则可以使得企业更为放心地对数据进行挖掘和利用,从而更好地发挥数据与信息在市场配置中的作用。

在实践中,这种数据财产化或商品化的做法已经被企业广泛采用,企业收集、储存与分析、出售个

---

〔77〕 Jeff John Roberts, "Google Shows Sites That Get Most 'Right to Be Forgotten' Requests, More than 500K Pages Removed", Fortune (Nov. 24, 2015, 10:37 AM), http://fortune.com/2015/ 11/24/google-forgotten-data/, accessed October 5, 2017.

〔78〕 第20条第1段。

〔79〕 对此的一个分析,参见 Peter Swire & Yianni Lagos, "Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique" 72 *Md. L. Rev*. 335(2013).

〔80〕 参见 Lorrie Faith Cranor, "Necessary But Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice" 10 *J. TELECOMM. & HIGH TECH. L*. 273 (2012).

〔81〕 Omri Ben-Shahar & Carl E. Schneider, "The Failure of Mandated Disclosure" 159 *U. PA. L. REV*. 647, 671 (2011).

〔82〕 对于这种经典自由主义法哲学的辩护,参见 Richard A. Epstein, *Simple Rules for a Complex World*, Harvard University Press, 1995.

人数据,这已经成为了一种常态。[83]尤其在美国和中国这样的隐私保护标准相对较低的国家,互联网企业对于数据的大规模收集与处理已经成为其核心竞争力之一,而这些企业也经常将这种收集的数据视为自身的核心财产。在很多企业看来,以财产权的进路来对待数据隐私,这既可以保护消费者,将选择权交给消费者个体,又可以促进企业合理地发挥大数据的作用。[84]

但另一方面,已经有很多学者与评论者指出,基于同意与传统财产权保护的进路则可能面临对个人数据保护不足的问题。莱西格等人曾经主张赋予个人数据隐私以财产权,认为这种赋权有助于个人在和互联网公司的博弈中掌握更多筹码,从而维护自身利益。但现实是,基于种种原因,个人往往难以实现对自身隐私权益的维护。

首先,个人可能没有能力理解网站等数据收集者的隐私政策。网站的隐私政策往往非常专业,即使是专业性的学者,要想完全理解可能都需要花费很大精力。就更不用说一般读者了,一般读者在面对此类隐私政策时,往往是一头雾水,难以对其进行准确判断。其次,在面对隐私政策时,普通人也很可能会对风险发生误判,对于其中存在的隐私风险认识不足。行为主义的大量研究告诉我们,人们往往会对直接产生重大风险的事项具有警觉性,而对于由信息泄露所产生的风险,人们往往会认识不足。[85]最后,普通人也不太可能有时间和精力完成对隐私政策的阅读与理解,正如一项研究所指出的,一个美国公民,如果要阅读所有访问网站的隐私公告,那么他一年可能需要花费高达 244 个小时的时间。[86]

总之,基于财产权的隐私保护虽然具有优点,但也有着不可避免的弊端。由于以上提到的种种原因,个体在面临信息收集、储存、处理与披露时往往很难做出真正理性的判断,从而也很难对相应的风险进行相应的防范。在大数据时代,情形就更是如此,风险与信息的关系可能并非一一对应,某一次信息收集、处理与披露可能不会立即带来风险,但这些信息一旦被集合,就会产生风险的“聚合效应”(aggregation effect)。[87]特别是当这些信息被某些犯罪分子掌握,即使这些信息是碎片化的,也可能会带来意想不到的风险。[88]

四、数据隐私的重新思考:消费者预期与风险规制

对于隐私人格权保护与财产权保护的弊端,《条例》并非完全无视,如果我们再次全面分析《条例》,会发现其中有些条款其实提供了解决传统隐私保护的一些方式。与传统的人格权进路或财产权

〔83〕 参见 Jessica Litman, “Information Privacy/Information Property” 52 *Stan. L. Rev*. 1283 (2000).

〔84〕 一个例子是 Facebook,其主管明确接受了施瓦茨等学者提出的数据隐私财产权保护的观念。参见 Timothy D. Sparapani, “Putting Consumers at the Heart of the Social Media Revolution: Toward a Personal Property Interest to Protect Privacy” 90 *N. C. L. Rev*. 1309, 1313 (2012).

〔85〕 Alessandro Acquisti & Jens Grossklags et al., “What Can Behavioral Economics Teach Us About Privacy?” in Acquisti A. , Vimercati S. C. , Gritzalis S. , Lambrinoudakis C.ed., *Digital Privacy: Theory, Technologies and Practices*, Auerbach Publications (Taylor and Francis Group), 2007, p. 363.

〔86〕 Lorrie Faith Cranor, “Necessary But Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice”, 10 *J. TELECOMM. & HIGH TECH. L*. 273, 274 (2012).

〔87〕 参见 Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age*, New York University Press, 2004, pp.44-47.

〔88〕 最近发生的徐玉玉诈骗案就是一个典型的案例,来源:https://baike.baidu.com/item/8•19 徐玉玉电信诈骗案 /20091304?fr=aladdin,2017 年 10 月 5 日访问。

进路不同,这些条款更多地以语境化的消费者预期和风险规制的视角来看待数据隐私的保护。

首先,《条例》虽然强化了个人同意作为数据收集与处理的基石,但《条例》也意识到,“同意”本身是一个非常含混的概念,很多时候,判断数据主体是否“同意”,其实更多是判断在某个特定语境之下,消费者对其个人数据的收集与处理是否存在合理预期。[89]例如,《条例》规定,当数据主体没有明确表示同意,判断数据处理是否合法,应当考虑“个人数据收集时的目的与计划进一步处理的目的之间的所有关联性”;[90]及“个人数据收集时的语境,特别是数据主体与控制者之间的关系”。[91]而欧洲议会与欧盟理事会对于《条例》的重述也指出,对于数据控制者是否存在收集与处理的正当利益,需要评估“数据主体在收集个人数据的语境中,是否可以合理地预期是否会基于此种目的而进行数据处理”。如果“数据主体一般没有预期会有进一步数据处理的情形下,数据主体的利益和基本权利优先于数据控制者的权利”。[92]

其次,对于数据收集、储存、处理与披露可能带来的风险,《条例》也从各个层面规定了风险预防与风险规制。例如,《条例》第 32 条规定了与风险相称的技术与组织措施:“在考虑了最新水平、实施成本、处理的性质、处理的范围、处理的语境与目的之后,以及处理给自然人权利与自由带来的伤害可能性与严重性之后,控制者和处理者应当采取包括但不限于如下的适当技术与组织措施,以便保证和风险相称的安全水平。”第 35 条规定了风险评估:“当某种类型的处理——特别是适用新技术进行的处理——很可能会对自然人的权利与自由带来高风险时,在考虑了处理的性质、范围、语境与目的后,控制者应当在处理之前评估计划的处理进程对个人数据保护的影响。”[93]第36条规定了监管机构的风险监管,当监管机构认为,某些“预期的处理将违反本条例,特别是当控制者无法识别或减小风险,监管机构应当在收到咨询请求的八个星期以内向控制者以及——在适用的情况下——处理者提供书面建议”而且可以运用相应的权力进行应对。[94]

相比起上文提到的数据隐私的人格权与财产权保护,可以说《条例》所包含的消费者预期与风险规制进路更为合理地回应了网络与大数据社会中的隐私保护。

第一,这种进路可以避免因为个人同意而造成的个人数据无法被合理地二次使用,从而错过大数据时代信息合理使用所带来的红利。在大数据时代之前,全球范围内的隐私规范主要在于让人们自主决定是否、如何以及经由谁来处理他们的信息,具体来说就是“告知和许可”公式化系统来设定隐私条款。但大数据时代的重要特征就在于数据的全体性、混杂性和相关性,数据往往需要被积淀和二次利用,才能发挥其效益。在这种前提下,“因为数据的价值很大一部分体现在二级用途上,而收集数据时并未作这种考虑,所以‘告知与许可’就不能再起到好的作用了”。[95]

第二,消费者预期进路可以更好地确定个人数据保护的合理边界与促进信息的合理流通。正如

---

〔89〕 例如,在自动驾驶的场景中,要求自动驾驶车辆获取路边行人同意收集其个人数据,显然是极其荒谬的。

〔90〕 第 6 条第 4 段(a)。

〔91〕 第 6 条第 4 段(b)。

〔92〕 Recitals of GDPR, https://gdpr-info.eu/recitals/no-47/, accessed October 5, 2017.

〔93〕 第 35 条第 1 段。

〔94〕 第 36 条第 2 段。

〔95〕 舍恩伯格指出,大数据时代的隐私保护模式“应该更着重于数据使用者为其行为承担责任,而不是将重心放在收集数据之初取得个人同意上。这样一来,使用数据的公司就需要基于其将对个人所造成的影响,对涉及个人数据再利用的行为进行正规评测”。参见[英]维克托·迈尔—舍恩伯格、肯尼斯·库克耶:《大数据时代:生活、工作与思维的大变革》,盛杨燕、周涛译,浙江人民出版社 2013 年版,第 220 页。

上文所述,无论是开放性的人格权还是以同意为核心的财产权,都难以为数据收集与处理提供较为合理的合法性边界,因为二者都以形式主义的观点来看待个人数据的保护问题,都把个人数据保护问题视为一个脱离语境的一般性规则问题。但无疑个人数据保护与流通是一个高度场景化或语境化的问题。在这一点上,消费者预期的进路可以结合具体的生活场景,在具体生活场景与社会关系中思考个人数据保护的边界,从而更好地确定信息保护的合理边界与信息的合理流通。

最后,从风险规制的角度来看,无论是数据隐私的人格权保护还是财产权保护,都不足以对风险进行预防与规制,因为在网络时代特别是大数据时代,数据风险已经成为一个系统化、复杂化的问题,个人已经很难对风险做出一次性的合理判断。这也就是说,通过法律对个人数据进行一次性的救济——无论这种救济是基于人格权还是财产权——可能都不足以对伴随数据收集、处理与流通中的风险进行规制。要对伴随数据收集、处理与流通中的风险进行规制,就必须全方位地对相关风险进行预防、评估与救济。

如果我们将目光投向大洋彼岸,会发现美国在《条例》草案出台前后所拟的隐私法案更多强调了这一消费者合理预期与风险规制的进路。2012 年,当时的奥巴马政府为了回应《条例》,出台了《消费者隐私权利法案》(Consumer Privacy Bill of Rights)。如同其名称所表明的一样,这个法案以消费者这一概念作为消费者保护的基本概念,而且,在其他要求之外,该法案将尊重语境(respect for Context)和安全(security)作为其核心要素。就尊重语境来说,其将“消费者有权期望机构以和消费者提供数据的语境相一致的方式来收集、使用和披露个人数据”作为法案的核心;就安全来说,其将“消费者有权确保对其个人数据的处理是安全和负责任的”作为法案的核心。[96]

从数据隐私的原理来说,我们可以发现这一进路其实更符合数据隐私的特征。在传统的隐私理论中,隐私保护是一种典型的私权,隐私意味着某种确定性的个人空间,保护隐私是因为隐私为个人提供了这种独处的空间、为人格发展提供了保障。[97]但是,近几十年来,一些较为前沿的隐私理论已经指出,隐私恰巧必须放在社群的语境中才能被充分理解,因为个人的合理空间或个人人格都是由社会构成的,只有在社群共同体中,个人的合理空间或人格才具有实现的可能。[98]

对于个人数据来说,如果一个社群具有较为合理的信息与数据流通机制,那么侵犯隐私的情形就会大大降低。因为在这种社会中,信息的流通机制将会大致符合人们的日常预期。如果说现代计算机与网络社会的兴起对隐私造成了很大的威胁,这主要是因为计算机与网络社会改变了原先社群的信息流通机制,而其自身尚未建立其具有语境公道性(contextualized integrity)的信息流通方式。[99]在这种背景下,信息与数据的流通方式就有可能脱离人们的预期,就有必要通过法律来对信息流通方式进行合理的规制,以促进数据在各种语境下能够合理流通,同时保障伴随数据合理流通的风险能够

---

〔96〕 Office of the Press Secretary, “We Can’t Wait: Obama Administration Unveils Blueprint for a ‘Privacy Bill of Rights’ to Protect Consumers Online”, https://obamawhitehouse.archives.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights, accessed October 5, 2017.

〔97〕 例如 Samuel D. Warren & Louis D. Brandeis, “The Right to Privacy” 4 *Harv. L. Rev*. 193 (1890).

〔98〕 Robert C. Post, “The Social Foundations of Privacy: Community and the Self in the Common Law Tort” 77 *Cal. L. Rev*. 957, 962 (1989). 波斯特的社会人格理论基础是当时其伯克利大学社会学系的同事厄文戈夫曼(Erving Goffman)的理论,参见 E. Goffman, “The Nature of Deference and Demeanor”, in *Interaction Ritual: Essays on Face-to-Face Behavior*, New York: Doubleday,1967, p. 47; E. Goffman, *Relations in Public: Microstudies of The Public Order*, Basic Books, 1971, pp. 28.

〔99〕 Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, 2009, p. 127.

得到有效规制。[100]

五、结语

本文对《一般数据保护条例》进行了较为全面的介绍,总结了《条例》的特征。通过这种介绍与总结,本文指出,《条例》从整体上采取了强化数据主体权利的立场,大大拓展了此前隐私法所赋予给数据主体的权利。其中的有些新型权利,例如被遗忘权与数据携带权,极大地改变现有的法律框架,并且会对企业与其他实体收集与使用数据产生重大影响。学界和实务界有必要对此进行进一步的研究,以更好地准备与回应这一变化。

通过对《条例》的介绍与总结探讨了数据隐私的性质与法律保护的框架,本文指出了《条例》暗含的数据隐私保护的两种框架:人格权保护与隐私权保护。通过分析这两种权利保护的利弊,本文认为,必须把数据权利、人格权、隐私权这些概念还原到特定的语境与社群中进行思考,一旦我们把这些概念还原到特定的语境和社群中,就会发现数据保护的核心在于使得数据与信息在具体的语境与社群中能够恰当地流动。因此,在判断《条例》或其他法律所赋予给数据主体的权利时,最重要的不在于试图抽象地界定某种权利的边界——无论这种权利是基于人格权还是财产权的。相反,重要的在于将权利还原到具体的语境与社群中,在具体的语境与社群中判断人们的预期与权利的边界。

从具体的法律保护模式来说,这意味着对数据隐私的保护应当放在风险规制与消费者保护的框架下进行。一方面,相关监管机构应当对数据被泄露或误用的风险进行评估和监管,从公法的角度对相关风险进行监管;另一方面,应当积极调动公民个体的积极性,通过消费者法的保护框架帮助消费者或数据主体。对于数据的收集、处理、储存与披露,应当要求相关数据收集者、控制者或处理者承担相应的透明性义务,应当保证消费者尽可能真实和准确地了解相应的风险,包括财产损失、人身伤害以及人格受损的风险。如此,消费者个体将能够更好地对自身的数据隐私进行自我管理,从而促进整个社会的数据与信息的合理流通。

(责任编辑:陆宇峰)

〔100〕 值得强调的是,《条例》本身也“欧盟内部个人数据的自由流动”视为其主要目标。例如,第 1 条“主要事项与目标”第 3 段规定:“在处理个人数据中保护自然人,这不应当对欧盟内部个人数据的自由流动进行限制或禁止。”