欧洲人权法院数据隐私权的保护机制*

管朝辉
（武汉大学　法学院，湖北　武汉　430072）

摘　要：为应对侵犯数据隐私权的情况，欧洲人权法院在“不干涉原则”的基础上，创设了“无支配原则”。“无支配原则”的形成原因有二：一是干涉行为本质发生变化，二是“无支配自由”理论更具说服力。借鉴欧洲人权法院数据隐私权的保护机制，我国数据隐私权的保护机制可以从两个方面完善：一是调整侵权行为和损害结果的证明标准，二是强化法官对合目的性和正当性的说理能力。

关键词：数据隐私权；欧洲人权法院；不干涉原则；无支配原则
中图分类号：D99　　**文献标识码**：A　　**DOI**：10.19358/j.issn.2097-1788.2023.06.003
引用格式：管朝辉. 欧洲人权法院数据隐私权的保护机制［J］. 网络安全与数据治理，2023，42(6)：15-20.

Protection mechanism of the European Court of Human Rights on data privacy

Guan Zhaohui
(School of Law, Wuhan University, Wuhan 430072, China)

Abstract: The European Court of Human Rights has created “non-domination principle” based on “non-interference principle”. The formation of “non-domination principle” has two reasons: the nature of the tort has changed and the “non-domination freedom” is convincing. Drawing on protection mechanism of the European Court of Human Rrights on date privacy, China can be improved from two ways: on one hand, the mechanism is to adjust the standard of proof of tort and damage, on the other, it is to strengthen the judge's reasoning ability to purposiveness and legitimacy.

Key words: data privacy; the European Court of Human Rights; non-interference principle; non-dominance principle

0　引言

随着信息技术的渗透，在物理空间外还产生了无限延展的虚拟空间[1]，人们在虚拟空间中所产生的个人信息、个人数据等，成为了数据隐私权的保护对象[2]。但在巨大的算力和无所不在的数据流面前，这种保护仍旧微不足道[3]。某些国家的法律赋予政府机构侵入公民计算机和其他设备的权力，某些大数据企业利用信息技术的不对称性收集、分析用户数据画像，某些不法分子利用数据漏洞实施窃取、非法转让个人数据的行为，最终导致公民的数据隐私暴露在公共互联网中[4]。对此，国际社会正在大力强化对数据隐私权的保护，并在地区、区域和国家层面形成相应的数据隐私权保护制度。

欧洲人权法院对数据隐私权的保护尤为严格。最初，欧洲人权法院在处理侵犯数据隐私权的案件时，采用了“不干涉原则”的人权保护机制[5]。但在大数据侵权和大规模监视出现的挑战下，欧洲人权法院又创设了“无支配原则”的人权保护机制，并成为欧洲人权法院保护数据隐私权的新趋势。本文在阐述“不干涉原则”和“无支配原则”运作模式及差异的基础上，分析“无支配原则”的产生原因，以期为我国数据隐私权的保护机制提出建议。

1　“不干涉原则”和“无支配原则”的运作模式及差异

欧洲人权法院始终强调《欧洲人权公约》（以下简称《公约》）在人权领域具有“欧洲公共秩序的宪法文书”的作用[6]。因此，欧洲人权法院在审理侵犯数据隐私权的案件时，坚持将《公约》作为裁判依据，通过对《公约》第8条进行解释，从而探索出更有利于保护数据隐私权的机制。时至今日，“不干涉原则”和“无支配原则”均出现在欧洲人权法院审理侵犯数据隐私权的案件中，为更好理解这两种机制的运作模式和差异，本文将通过两个判例加以说明。

*基金项目：国家社会科学基金重大项目（18ZDA149）

www.pcachina.com

1.1 “不干涉原则”的运作模式

“不干涉原则”的运作模式分为四步：首先，需要确定行为是否干涉了申请人的数据隐私权，主要根据申请人的申诉请求（含被侵权主体、具体侵权行为以及具体损害等）是否符合《公约》第8条的范围来判定，即第8条第1款：人人有权享有使自己的私人和家庭生活、家庭和通信得到尊重的权利。其次，需要确定干涉行为是否具有合法性，主要根据相关法律是否明确、是否具有可访问性和可预见性来判定。再次，需要确定干涉行为是否具有合目的性，主要根据干涉行为是否有利于保护国家、社会和公共利益来判定。最后，需要确定干涉行为是否具有正当性，主要根据干涉行为的目的与干涉行为对数据隐私权的影响是否满足比例原则、被侵权主体是否具有救济途径来判定。

以 Surikov v. Ukraine 案为例，此案中，申请人 Surikov 是某出版社员工，该出版社根据一份“申请人因精神病性障碍，被宣布为不适合在和平时期服兵役”的数据证明，拒绝将申请人晋升到与其资历相当的职位。申请人于是对出版社提起数据保护民事诉讼，地区法院驳回了申请人的诉讼请求。申请人后又向上诉法院和最高法院分别提起上诉和上诉许可申请，也均被驳回。申请人最后以乌克兰政府为被申请人，向欧洲人权法院提起申诉，认为雇主任意收集、保留和使用敏感、过时和不相关数据的行为，侵犯了自己的数据隐私权，涉嫌违反《公约》第8条。针对申请人的申诉理由，乌克兰政府辩称，根据乌克兰《兵役法》的规定，雇主有义务将军事身份证上载有的关于免除兵役的数据复制到人事记录上，因此关于申请人免除兵役的数据并非机密。

欧洲人权法院从以下四个方面对本案进行论证：首先，出版社依据《兵役法》所实施的收集、保留和使用关于申请人免除兵役的数据的行为，涉及申请人的健康数据隐私权，构成了对申请人私人生活的干涉，存在违反《公约》第8条的情形。因此，申请人的申诉属于欧洲人权法院的受案范围。其次，对申请人而言，《兵役法》的具体内容是明确的、可预见的，其中包含雇主有权利将免除兵役的数据信息复制到人事档案上。因此，干涉行为具有合法性。但是，干涉行为仅仅是为了判定申请人是否可以工作晋升，这显然与《公约》第8条第2款所规定的例外情形不符，根据《兵役法》的规定，收集、保留和使用数据的目的是为了维护国家安全，而非用于工作晋升的判定。因此，干涉行为在合目的性上没有依据。最后，干涉行为的目的与干涉行为对申请人数据隐私权的影响不满足比例原则，并没有平衡好雇主利益与申请人数据隐私权之间的关系，且干涉行为也没有为申请人提供必要的救济途径。因此，干涉行为在正当性上也没有依据。综上，欧洲人权法院认为，出版社收集、保留和使用关于申请人免除兵役的数据的行为，虽然具有合法性，但并不具备合目的性和正当性，因此违反了《公约》第8条，构成对申请人数据隐私权的侵犯。

1.2 “无支配原则”的运作模式

“无支配原则”的运作模式也分为四步：首先，需要确定行为是否可能干涉申请人的数据隐私权，主要根据申请人的申诉请求（含法律所规定的影响数据隐私权的措施、救济措施等）是否符合《公约》第8条的范围来判定。其次，需要确定干涉行为是否具有合法性，主要根据相关法律是否明确、是否具有可访问性和可预见性来判定。再次，需要确定相关法律是否具有合目的性，主要根据相关法律是否有利于保护国家、社会和公共利益来判定。最后，需要确定相关法律是否具有正当性，主要根据相关法律的具体规定，包括授权类型、授权条件、保障措施等是否满足比例原则来判定[7]。

以 Big Brother Watch and Others v. the United Kingdom 案为例，此案中，Big Brother Watch 等申请人认为，“斯诺登事件”揭露了美国和英国情报部门所实施的电子监视计划，而申请人自身的数据通信活动也很有可能被英国情报部门截获或者从相关通信服务提供商处获取。申请人于是以英国政府为被申请人，向欧洲人权法院提起申诉，认为英国情报部门所实施的电子监视行为属于对数据隐私的秘密监视，侵犯了其数据隐私权，涉嫌违反《公约》第8条。针对申请人的申诉理由，英国政府辩称，政府依据的是《调查权监管法案》中规定实施的数据监视行为，该行为无法进行大规模数据拦截，且所获取的数据信息会有选择性地打开和保留，因此申请人的数据隐私权并未受到侵害，尤其是申请人也无法提供证据。

欧洲人权法院在处理本案时做出了不同的论述。首先，欧洲人权法院认为，尽管申请人没有证据证明自己的数据隐私权受到了秘密监视的影响，但如果满足以下两个条件的话，申请人仍然可以声称自己是秘密监视行为的受害者：一是秘密监视行为的对象包括申请人；二是国家没有提供有效救济。对于第一个条件，法院将对法律所规定的影响数据隐私权的措施进行考察，确定申请人是否可能受到影响，如果所有人或者申请人属于该措施所针对的群体，申请人就可能受到影响；针对第二个条件，法院将根据国家救济措施的可获取性和有效性，来判定是否存在有效救济，如果国家并没有向怀疑自己的数据隐私权可能受到影响的人提供有效救济，申

www.pcachina.com

请人有权担忧其数据隐私权受到侵犯。在本案中，尽管申请人无法证明自己的数据隐私权受到批量截获的影响，但英国的数据截获行为所针对的对象是不特定境内外公民，且随着截获程度的增加，数据隐私权所受干扰会更加严重，因此可以推定申请人是数据截获行为的受害者，数据截获行为可能涉及申请人的私人生活数据隐私，可能构成对申请人私人生活的干涉，存在违反《公约》第 8 条的情形。其次，欧洲人权法院认为，英国政府实施数据截获行为所依据的《调查权监管法案》是明确的、可预见的。一方面，《调查权监管法案》第 6.4 条明确说明了政府将在何种情况下进行数据截获和数据共享；另一方面，《调查权监管法案》已经公开发表，因此干涉行为具有合法性。再次，欧洲人权法院放弃对干涉行为合目的性和正当性的论证，转而论证相关法律的合目的性和正当性。欧洲人权法院认为，《调查权监管法案》所追求的目的是保护国家安全、防止混乱和犯罪以及保护他人的权利和自由，这与《公约》第 8 条第 2 款所规定的例外情形相符，因此相关法律具有合目的性。最后，欧洲人权法院对相关法律的正当性表示担忧，在对《调查权监管法案》进行严格分析后，认为“截获数据的行为（在当今社会下）很可能被滥用，并对个人数据隐私权产生不利影响。尽管《调查权监管法案》提供了强有力的保障措施……但是这些措施在授权、可行性、监督等方面并不足以弥补对公民所造成的影响。”因此相关法律不具备正当性。综上，欧洲人权法院认为，英国政府截获数据的行为具有合法性，其所依据的《调查权监管法案》具有合目的性但不具有正当性，因此违反了《公约》第 8 条，构成对申请人数据隐私权的侵犯。

1.3 “不干涉原则”和“无支配原则”的差异

从“不干涉原则”和“无支配原则”的运作模式中可以总结出两点差异：一是在判定某一行为是否干涉数据隐私权时，“不干涉原则”的认定标准较“无支配原则”高。“不干涉原则”要求行为真实地干涉了数据隐私权，因此申请人需要证明被侵权主体、具体侵权行为以及具体损害等要件；“无支配原则”不要求行为真实地干涉数据隐私权，仅有干涉的可能性即可，因此申请人只需证明法律所规定的影响数据隐私权的措施是针对当事人的，以及国家没有提供有效救济。二是在认定合目的性和正当性上，“不干涉原则”和“无支配原则”的认定对象不同。“不干涉原则”是对干涉行为的合目的性和正当性进行认定，而“无支配原则”是对干涉行为所依据的相关法律的合目的性和正当性进行认定。

2 “无支配原则”的产生原因

2.1 现实原因：大数据使干涉行为的认定标准失效

权利受到干涉，是欧洲人权法院受理案件的前提。在具体的数据隐私权侵权案件中，因为干涉行为通常涉及明确的时间、地点和人物，申请人只要能够自证为被侵权主体，并且指明侵权主体和具体侵权行为，欧洲人权法院便可以认定申请人的数据隐私权受到了干涉[8]。但是，随着大数据技术的进步，数据侵权行为开始变得隐蔽且难以认定。以城市街道的闭路电视摄像机为例，由于拍摄采集的随机性，个人作为偶然因素会被记录在内形成数据，当事人常常意识不到自己的数据信息正在被收集，即使意识到也不可能亲自检查所有数据流是否包含其数据。假设当事人意识到且有能力去检查所有数据流，核心问题转变为当事人如何去证明自己的权利受到了具体损害。因为数据信息在经过大数据处理后，可能会从单纯的数据信息变成宏观的政策决策并最终呈现在大众面前，而当事人很难证明这一政策决策对个人利益的损害。因此，“不干涉原则”下的干涉行为认定标准就可能失灵。

如何在当事人无法证明具体侵权行为和具体损害的情况下认定当事人的数据隐私权受到干涉，“无支配原则”选择放宽对干涉行为的认定标准，仅需行为满足可能干涉数据隐私权。究其原因，是侵犯数据隐私权的行为的本质发生了变化，从对个人数据隐私权的具体侵犯转向对数据所有人权利结构的侵犯[8]。大型科技公司和政府机关利用大数据技术优势，获取海量公民数据信息并建立起大型数据库，与公民处于完全不对等的地位。而想要保护数据隐私权的公民，又限于侵权行为过于隐蔽且没有办法证明具体损害。因此一旦继续沿用“不干涉原则”的干涉行为认定标准，就意味着要放弃对大规模秘密监视行为、数据保留行为等侵犯公民数据隐私权的行为的司法审查，这显然不符合欧洲人权法院对隐私权保护的要求。因此，欧洲人权法院放宽对干涉行为的认定标准，采用“无支配原则”，认为行为只需存在干涉数据隐私权的可能即属干涉行为。此举降低了申请人的举证难度，可以避免当大规模侵犯数据隐私权的隐蔽行为发生时申请人走投无路。

2.2 理论指引：“无支配自由”保障权力不被滥用

“不干涉原则”是自由主义中的“不干涉自由”在数据隐私权中的运用。密尔在其文章中提到，只要个体的选择对他人没有产生任何有害影响，社会就不应当干涉其选择[9]。因此，只有当存在具体的干涉行为并导致实际损害时，才可以认定当事人的数据隐私权受到了侵犯。

www.pcachina.com

而且，干涉行为对他人数据隐私权所产生的损害并非都是不可接受的，在个人数据隐私权需要让位于更高层面的国家、社会和公共利益，且为个人数据隐私权已经提供保障的情况下，也可以排除干涉行为对他人数据隐私权的侵犯。因此，审查干涉行为的合目的性和正当性就成了确定干涉行为是否侵犯数据隐私权的必要环节。然而，大数据技术的进步，使得当事人通常无法证明具体的侵权行为以及具体损害。尽管“无支配原则”放宽了干涉行为的认定标准，但改变后的“可能对数据隐私权造成影响”的标准表明了欧洲人权法院并没有把握确定是否存在干涉行为。如果在后续的论证过程中坚持“不干涉原则”的论证框架，对不确定的干涉行为的合目的性和正当性进行论证以确定当事人的数据隐私权是否受到侵犯，那么欧洲人权法院所得的结论将建立在一个不牢固的基础之上，容易被他人诟病。

放弃对具体干涉行为的关注，着眼于权力关系和潜在的权力滥用，是欧洲人权法院探索出来的路径，也是共和主义的“无支配自由”在数据隐私权中的运用，即“无支配原则”。纽威在其文章中说道，在没有其他实体实际干涉他人活动的情况下，个人都是自由的。“无支配自由”取消了实际干涉的要求，而侧重于消除他人任意干涉的危险或潜在危险；“无支配自由”更关注通过减少支配和任意干涉，来确保人民的自制能力[10]。在现实中，“无支配自由”并不过多关注他人是否真正行使了权力，是否实施了具体干涉，而是关注他人的权力范围以及是否有足够的保障措施来防止权力的任意行使。相应转化到“无支配原则”上，判定当事人的数据隐私权是否受到侵犯，即去关注可能的干涉行为所依据的相关法律的合目的性和正当性。一方面，需要考虑相关法律制定的目的是否有利于保护国家、社会和公共利益；另一方面，需要考虑相关法律的具体规定，包括授权类型、授权条件、授权范围、保障措施等是否满足比例原则。如果不满足上述两个条件，那么就可以说权力被任意行使了，当事人的数据隐私权受到了侵犯。“无支配原则”绕过对干涉行为合目的性和正当性的论证，转而去讨论确定的法律的合目的性和正当性，进而明确权力是否任意行使，并作为认定公民数据隐私权是否受到侵犯的依据。此种论证逻辑相较于“不干涉原则”而言更具有说服力，因此越来越多的数据隐私权学者主张在此类案件中适用“无支配原则”。[8]

3　对中国数据隐私权的保护机制的借鉴意义

建设数字中国，是数字时代推进中国式现代化的重要引擎，是构筑国家竞争新优势的有力支撑[11]。数据作为建设数字中国的核心要素，加强对数据隐私权的保护，是实现数字中国建设的必由之路。欧洲人权法院数据隐私权的保护机制相对成熟，为各成员国公民的数据隐私提供了有效保护[12]。因此，通过对欧洲人权法院数据隐私权的保护机制进行扬弃，可为我国数据隐私权的保护机制的完善提供借鉴。

3.1　类型化设计：调整侵权行为和损害结果的证明标准

欧洲人权法院数据隐私权的保护机制的第一个特点，是对数据隐私权干涉行为的认定标准采取了类型化设计：一是针对有具体被侵权主体的侵犯数据隐私权的案件，如 A 公司、B 政府实施对某一特定主体 C 的数据收集、保留和使用等行为，欧洲人权法院采用“不干涉原则”，要求申请人证明具体的侵权行为和损害结果；二是针对无具体被侵权主体的侵犯数据隐私权的案件，如 A 公司、B 政府实施对某群体 D、所有公民 E 的大规模秘密监控、截获数据等行为，欧洲人权法院采用“无支配原则”，在可能影响数据隐私权的行为是针对当事人的情况下，推定存在侵权行为和损害结果。欧洲人权法院之所以进行类型化设计，而不是全盘适用新发明的“无支配原则”，是因为“不干涉原则”本就对具体侵犯数据隐私权的案件有适用性，如果欧洲人权法院将所有关于数据隐私权的案件都适用“无支配原则”，那么不属于侵权行为所针对的公民，就会借用欧洲人权法院放松对干涉行为认定标准的机会，假借自身数据隐私权可能受到侵犯，要求欧洲人权法院受理，最终造成无关案件的出现。

目前，我国法院在审理侵犯数据隐私权的案件时，采用的是统一的证明标准。在立法上，我国有关数据隐私权的法律，如《网络安全法》《数据安全法》《个人信息保护法》《民法典》侵权责任编等，均未对侵犯数据隐私权的证明责任分配提供特殊保护；在司法上，法院严格遵循要件构成的审理思路，通过对侵权行为、损害结果、因果关系和主观过错进行认定，从而确定侵权主体所承担的责任[5]。因此，被侵权主体需要根据《民事诉讼法》第六十七条的规定，举证证明具体的侵权行为和损害结果。这种统一的证明标准通常仅适用于具体侵犯数据隐私权的案件。但是，对于大规模侵犯数据隐私权的案件，由于侵权行为隐蔽、针对对象模糊，因此被侵权主体在举证时存在困境，难以证明侵权行为和损害结果，最终容易陷入败诉的局面。例如在“顾某与奇智软件（北京）有限公司、北京奇虎科技有限公司隐私权纠纷案”“丁某某与深圳市腾讯计算机系统有限公司隐私权纠纷案”中，原告均主张被告存在收集、使用其数据的行为，构成对其数据隐私权的侵犯，但法院均以证据不足以证明存在具体侵权行为和损害结果为由，不予支持

www.pcachina.com

原告诉讼请求。如果对此还采取与具体侵犯数据隐私权的案件相同的证明标准，那么被侵权人自始至终将处于弱势地位。

因此，有必要借鉴欧洲人权法院数据隐私权的保护机制，对中国数据隐私权侵权行为和损害结果的证明标准进行类型化处理：在处理有具体被侵权主体的侵犯数据隐私权的案件时，要坚持要件构成的审理思路；在处理无具体被侵权主体的侵犯数据隐私权的案件时，可以借鉴“无支配原则”中对干涉行为和损害结果的推定方法，推定当事人是否属于被侵权主体，是否存在具体侵权行为和损害结果。这种推定的证明标准适用于民事、行政和刑事诉讼中，仍需要在有关数据隐私权的法律中作出明确规定。

3.2 运用比例原则：强化法官对合目的性和正当性的说理能力

欧洲人权法院数据隐私权的保护机制的第二个特点，是对合目的性和正当性的认定贯彻比例原则的说理：在“不干涉原则”中，欧洲人权法院通过运用比例原则，论证干涉行为的目的与干涉行为的影响之间的关系、干涉行为的救济与干涉行为的影响之间的关系，从而认定干涉行为是否合目的、是否正当；在“无支配原则”中，欧洲人权法院通过运用比例原则，论证相关法律制定的目的与推定的干涉行为的影响之间的关系、相关法律制定的保障措施与推定的干涉行为的影响之间的关系，从而认定相关法律是否合目的、是否正当。欧洲人权法院之所以要贯彻比例原则的说理，是因为尽管干涉行为或者推定的干涉行为所依据的相关法律都是在合法性的基础上限制公民的基本权利（如数据隐私权），但是社会发展的速度往往会超越法律制定的节奏[13]，因此法院可以发挥司法能动性，通过运用比例原则进行说理来约束干涉行为，平衡各方利益并解决社会问题。

目前，我国对使用公民数据隐私的目的、保障措施等作出法律规定。就使用公民数据隐私的目的而言，《网络安全法》第四十一条规定，网络运营者收集、适用个人信息，应当遵循合法、正当、必要的原则。《数据安全法》第二十八条规定，开展数据处理活动，应当有利于促进经济社会发展，增进人民福祉，符合社会公德和伦理。第三十二条规定，任何组织、个人收集数据，应当采取正当方式。《个人信息保护法》第五条规定，处理个人信息应当遵循正当、必要原则。第六条规定，处理个人信息应当具有明确、合理的目的，并且个人信息应当与处理目的直接相关。第十三条规定了个人信息处理者处理个人信息的六种情形，如为应对突发公共卫生事件、为公共利益实施新闻报道等。就使用公民数据隐私的保障措施而言，《网络安全法》规定，网络运营者在收集用户信息时，应当向用户明示并取得同意、应当建立报告制度。《数据安全法》规定，要建立数据分类分级保护制度、全流程数据安全管理制度、重要数据定期风险评估等。《个人信息保护法》确立了个人一般信息和个人敏感信息两类，明确数据处理者的告知义务、安全保护义务，数据监管部门的保护职责和监管职责。从上述法律规定中可见，我国数据隐私权的保护机制在立法中已经体现出比例原则，这为在数据隐私权案件审判中运用比例原则对侵权行为合目的性、正当性的说理提供指引。但是，针对公民数据隐私权问题，“言多必失”的思想普遍阻碍司法能动性的发挥[14]，主动运用比例原则来处理新场域下的数据隐私侵权行为合目的性、正当性问题仍较为少见。

因此，需要强化司法对我国数据隐私权侵权行为的合目的性和正当性的说理能力：第一，尽管我国不是判例法国家，但是指导性案例所体现的审理思路仍然值得借鉴，尤其是在数字中国建设期间，大规模收集用户个人敏感数据而导致的案件可能会大量出现。第二，重视数据隐私侵权行为与公共利益保护的关系说理。个人数据隐私和公共利益都是重要法益，两者需要兼顾而非偏废。例如面对严重损害国家安全利益的情况，即使采取大规模数据收集行为也不必然导致数据隐私权受侵犯；面对数字中国建设过程中企业或者组织大规模采集公民数据隐私的情况，就必须要明确采集的是何种数据隐私及其必要性。第三，重视数据隐私侵权行为与数据隐私保障措施的关系说理。欧洲人权法院在面对大规模监视的新场域下，通过说理的方式提高了数据隐私保障措施的要求[15]。我国在以《网络安全法》《数据安全法》《个人信息保护法》所提供的保障措施的基础上，应当根据具体的侵权行为来提高或者降低保障措施的要求。以数据保留时间为例，大数据企业为分析用户行为而大规模采集公民数据隐私的数据保留时间，应当小于国家为建设数字政府、数字法院等而大规模采集公民数据隐私的数据保留时间。

需要注意的是，欧洲人权法院在审查相关法律的合目的性和正当性时，有学者批评指出，欧洲人权法院在“无支配原则”中审查法律的行为与西方国家的宪法法院相似，但欧洲人权法院自身审查和评估法律的权力并没有在《欧洲人权公约》中进行规定，也没有其他任何法律依据，因此，这种权力缺乏合法性。我国法院在说理中一定要以法律为基础，专注于对法律本身进行解释。

4 结论

在大数据侵权和大规模监视的挑战下，侵犯数据隐

www.pcachina.com

私权的行为变得更加隐蔽。受“不干涉自由”和“无支配自由”的影响，欧洲人权法院通过运用“不干涉原则”和“无支配原则”，分类分步审理侵犯数据隐私权的案件，结合具体案情，根据比例原则定性、定量平衡利益，最终保护公民的数据隐私权不受个人、企业和国家的侵犯。在我国司法实践中，法院严格遵循要件构成的审理思路来处理侵犯数据隐私权的案件，这实际并不适用于大规模侵犯公民数据隐私权的情形，容易造成被侵权主体举证困难因而陷入败诉困境。欧洲人权法院数据隐私权保护机制对我国具有一定的借鉴意义，应以其为正反例，考虑调整侵权行为和损害结果的证明标准，强化法官司法说理能力，将比例原则作为司法审判工具，确保在大数据技术飞速发展的进程中，法院能够回应社会需求，从而推动我国数据隐私权保护机制的进步。

参考文献

[1] 马长山. 数字时代的人权保护境遇及其应对［J］. 求是学刊，2020（4）：103－111.

[2] 迈克尔·施密特等. 网络行动国际法塔林手册 2.0［M］. 黄志雄，译. 北京：社会科学文献出版社，2017.

[3] GENDEREN R. Privacy and data protection in the age of AI and robotics［J］. European Data Protection Law Review，2017（3）：3/

[4] 龚子秋. 公民“数据权”：一项新兴的基本人权［J］. 江海学刊，2018（6）：157－161.

[5] 李艳华. 欧洲健康数据的隐私保护机制及其对我国的启示——以《欧洲人权公约》第 8 条相关判例为视角［J］. 网络信息法学研究，2021（2）：181－211，297.

[6] DOUGLASSCOTT S. Bosphorus hava yallari turizm ve ticaret anonim sirketi v. Ireland［J］. Common Market Law Review，2006，43（1）：243－254.

[7] SLOOT B . A new approach to the right to privacy，or how the European Court of Human Rights embraced the non-domination principle［J］. Computer Law & Security Review，2018，34（3）：539－549.

[8] ［荷］巴特·范德·斯洛特等. 大数据时代隐私权保护的新路径——欧洲人权法院对“无支配原则”的适用［J］. 国际法学刊，2021（1）：139－148.

[9] ［英］约翰·密尔. 《论自由》［M］. 许宝骙，译，北京：商务印书馆，2005.

[10] NEWELL B C. The massive metadata machine：liberty，power，and secret mass surveillance in the U. S. and Europe［J］. A Journal of Law and Policy，2014（10）：514.

[11] 中华人民共和国中央人民政府. 中共中央 国务院印发《数字中国建设整体布局规划》［EB/OL］.（2023－02－27）［2023－03－04］. http：//www. gov. cn/zhengce/2023－02/27/content_5743484. htm.

[12] 田旭. 欧盟个人数据保护法的全球影响成因与启示［J］. 江西财经大学学报，2020（4）：135－147.

[13] 宋远升. 司法能动主义与克制主义的边界与抉择［J］. 东岳论丛，2017（12）：147－155.

[14] 凌斌. 法官如何说理：中国经验与普遍原理［J］. 中国法学，2015（5）：99－117.

[15] 吴常青. 欧洲人权法院为大规模监控建立新的审查标准［J］. 信息安全与通信保密，2022（8）：145－150.

（收稿日期：2023－02－20）

作者简介：

管朝辉（1998－），男，硕士研究生，主要研究方向：网络空间法、国际人权法。

（上接第 14 页）

[21] 申卫星. 论数据用益权［J］. 中国社会科学，2020（11）：110－131，207.

[22] 周小明. 信托制度：法理与实务［M］. 北京：中国法制出版社，2012.

[23] 龙卫球.《个人信息保护法》的基本法定位与保护功能——基于新法体系形成及其展开的分析［J］. 现代法学，2021，43（5）：84－104.

[24] 蔡丽楠. 数据信托参与数据治理：理论逻辑与实现机制［J］. 金融评论，2022，14（1）：66－79，123.

[25] 申卫星. 数字权利体系再造：迈向隐私、信息与数据的差序格局［J］. 政法论坛，2022，40（3）：89－102.

[26] 赵廉慧. 作为民法特别法的信托法［J］. 环球法律评论，2021，43（1）：68－84.

[27] 包晓丽，齐延平. 论数据权益定价规则［J］. 华东政法大学学报，2022，25（3）：64－79.

[28] VEN M V D，ABBAS A E，KWEE Z，et al. Creating a taxonomy of business models for data marketplaces［C］//34th Bled eConference. University of Maribor Press，2021.

[29] 张小松. 数据信托［J］. 中国科学基金，2021，35（3）：406－407.

（收稿日期：2023－04－04）

作者简介：

杨帆（1998－），女，硕士研究生，主要研究方向：计算法学。

www.pcachina.com

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

www.pcachina.com