Dispute Settlement 争议解决, 2023, 9(6), 3076-3082
Published Online November 2023 in Hans. https://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2023.96418

Hans汉斯

侦查中的大规模监控与个人信息保护

任灵春

中国海洋大学法学院，山东 青岛

收稿日期：2023年10月10日；录用日期：2023年11月7日；发布日期：2023年11月15日

摘　要

在大数据时代背景下，大规模监控在侦查中已经得到广泛运用，同时发挥着犯罪预防和犯罪侦查的作用，针对全社会大规模的监控与技术侦查措施不同，对不特定第三人进行监控也会对个人信息保护形成一定的挑战，信息共享和第三方理论的存在也会加剧这种冲突，为了平衡这一利益冲突，从个人信息保护的视角对大规模监控进行规制，以比例原则为宏观指导对大规模监控进行场景化的治理，通过权利保障和程序规则对其进行具体规制，同时也要注意个人信息保护的限度，不能一味强调个体赋权，以期实现犯罪治理和个人信息保护的平衡。

关键词

大规模监控，个人信息，侦查

Mass Surveillance and Personal Information Protection in Investigation

Lingchun Ren

Law School, Ocean University of China, Qingdao Shandong

Received: Oct. 10th, 2023; accepted: Nov. 7th, 2023; published: Nov. 15th, 2023

Abstract

In the context of the era of big data, mass surveillance has been widely used in investigation, while playing a role in crime prevention and crime investigation. Large-scale surveillance for the whole society is different from technical investigation measures, monitoring of an unspecified third party will also pose certain challenges to personal information protection, and the existence of information sharing and third-party theories will aggravate such conflicts. In order to balance this conflict of interest, large-scale surveillance should be regulated from the perspective of personal information protection. Large-scale surveillance should be governed in scenarios guided by the

文章引用: 任灵春. 侦查中的大规模监控与个人信息保护[J]. 争议解决, 2023, 9(6): 3076-3082.
DOI: 10.12677/ds.2023.96418

principle of proportionality, and specific regulation should be carried out through rights protection and procedural rules. At the same time, attention should be paid to the limits of personal information protection, rather than blindly emphasizing individual empowerment, in order to achieve the balance between crime management and personal information protection.

Keywords

Mass Surveillance, Personal Information, Investigation

1. 引言

从我国目前对个人信息法律保护状况而言，对于个人信息保护多在实体法领域进行规定，程序法方面并未过多涉及，可能是出于维护国家安全、社会公共安全的考量，为了保证执法机关的活动顺利进行，将刑事司法、执法领域中的个人信息干预行为作为例外，对其规制很少。在刑事诉讼中，侦查领域中大规模监控技术的运用对个人信息干预程度加深，但尚未纳入法律规制范围，不符合现代信息技术快速发展的要求，为此，本文将结合大数据时代的背景，对大规模监控在侦查中的用途进行梳理，揭示与技术侦查的不同之处，在分析数据共享和第三方理论对个人信息保护形成一定危险的基础上，为进一步寻求个人信息保护和犯罪治理的协调，基于保护个人信息的立场就如何规制大规模监控技术提出了自己的观点，即从坚持宏观的比例原则和具体的程序规则这两个方面进行规制。

2. 大规模监控在侦查中的运用

目前在公共领域中，随着现代信息和网络技术的发展，大规模监控的运用日益频繁，侦查机关基本实现了侦查领域中收集各类信息的大规模监控，以犯罪实施为节点讨论大规模监控的多种用途，对其进行性质判断，以便与技术侦查措施有更好的界分。

(一) 大规模监控在侦查中的用途

1) 犯罪实施前：预防、发现、制止犯罪

为了预防犯罪、防范社会风险，根据打击不法行为、保障公共安全的需要，公共领域中的大规模监控由此产生，在风险社会下，大规模监控技术在侦查中的广泛运用，会使得侦查提前介入到犯罪预备阶段，事先通过数据库信息的比对发现犯罪行为之间的隐性关系以此预防犯罪行为，对潜在犯罪者起到震慑的效果。[1]在犯罪实施前这一阶段，大规模监控通常发挥着预防犯罪的功能，一旦监控发现犯罪行为就会即时记录、存储这一信息，还可能会立即采取措施制止犯罪，这也说明大规模监控在这一阶段也具有侦查的功能，但是根据我国刑事诉讼的规范，立案才是侦查启动的前提条件，而在尚未发生犯罪时，侦查机关利用大规模监控技术进行监控只是起到预防犯罪、防控风险的作用，并未正式立案，所以这一阶段的大规模监控是否属于“侦查中”的作用是存在疑问的，因为监控的即时性使预防和侦查之间的界限变得模糊。[2]

2) 犯罪实施后：搜索犯罪嫌疑人等特定主体、收集证据材料

在犯罪发生后，侦查机关发现案件线索、寻求诉讼证据往往依赖于视频监控以此观察特定嫌疑人的行踪轨迹，收集与案件有关联的监控信息作为证据使用，然后进行整合描绘出完整的数字图像，从而锁

定犯罪嫌疑人。

大规模监控不仅仅包括公共场所中的视频监控，还涵盖网络空间的监控，在大数据背景下，侦查机关破案也更依赖于网络中存储的数据。在侦查过程中，司法机关利用第三方主体记录存储的数据进行侦查取证，由信息获取者到信息使用者实现了身份的转换。除了侦查机关即公权力机关进行大规模监控收集诉讼证据之外，非公权力机关也会基于商业用途实施大规模监控措施，比如网络服务商等第三方主体对公民提交至网络的各类信息实行监控，因为网络服务商有为刑事司法部门提供技术支持的责任，司法机关若获取了网络服务商的全部数据，这也说明对网络空间存储的数据实施了大规模监控，进而收集与案件相关的证据材料以查获犯罪嫌疑人、查明案件事实。

(二) 侦查中的大规模监控与技术侦查措施

侦查中的大规模监控与技术侦查措施其实是最为接近的，大规模监控收集个人信息同样具有封闭秘密的特征，侦查机关使用大规模监控技术对特定对象进行监控，这与技术侦查的构成要件是相同的，即适用对象的特定性、监控的技术性和秘密性，比如侦查机关对特定对象在公共场所运用大规模技术追踪其行踪等行为属于行踪监控技术侦查措施，对非特定主体进行监控以预防、发现犯罪和收集证据材料这一用途来说，就不符合技术侦查的构成要件。

两者最大的不同就是大规模监控适用的对象不特定，具有广泛性的特点，2012 年我国《刑事诉讼法》增设技术侦查一节，也是认识到了侦查机关的强制侦查措施对公民基本权利有所侵害的事实，将技术侦查的适用对象进行严格限制，只对特定案件的特定主体进行适用，但大规模监控的适用对象广泛，往往针对不特定对象，所以无法适用技术侦查的规定进行规制，并且也并未纳入刑诉法的规制范围，可能是因为还未认识到大规模监控会对公民权利造成侵害这一事实。如果要对大规模监控进行规制，首先需要判断大规模监控收集的公共领域中的个人信息是否也会侵害公民的隐私权？与相近技术侦查措施是否有相同的侵害性？个人将信息披露至网络，是否会丧失隐私权的保护？[3]只有确定大规模监控侵害了个人信息安全，才能谈如何规制的问题。

大规模监控在侦查中的运用也会促使传统侦查方式的转变，信息是宝贵的资源，是立案、侦查取证的重要线索，在大数据时代下更是如此，侦查中大规模监控的应用不同于以往传统侦查中遵循的“犯罪到立案再到侦查”这种先后顺序，不再只局限于一个物理空间，可以实现同步取证，侦查对象也更广泛，侦查模式从被动型、回溯型转向主动型、预防型，而且呈现一种信息前置的状态，即先通过信息的资源整合再进行后续的侦查工作。

3. 大规模监控对个人信息保护的挑战

为了维护国家安全、公共安全目的进行的针对全社会的大规模监控，所有人处于被全面监控的状态，与维护私益中的个人信息保护存在一定冲突，第三方理论和数据共享也对个人信息保护形成一定的挑战。

(一) 大规模监控与个人信息保护的冲突

长期以来，司法实务界基本上都认为大规模监控不会侵犯非特定对象的隐私权和个人信息安全，因为个人处于公共场所的行为不具有私密性，又基于“公共领域”规则——个人对身处公共领域从事的活动不具有隐私期待，公民可以调整自己在公共领域的行为，对于被监控也是处于知情状态，他们可能还会希望在公共场所安装摄像头以保障他们的安全。

但是在信息时代下，信息收集主体的多元化会引发全景式监控风险，[4]为了防控风险和预防犯罪，大规模的视频监控遍布于公共场所，尤其是在车站、机场、街道等人流量大、人群密集区域，公共场所的大规模监控是长期、密集的。公共空间又分为现实空间与网络空间，随着互联网技术的迅速发展，传统犯罪也渗入到了网络空间中，网络诈骗、网络赌博、网络恐怖主义等犯罪日益猖獗，为了防控违法犯

罪的风险，网络空间中的监控也基本全覆盖。网络监管从网络服务商细化到个人(网络服务商需要承担安全保障义务，个人也需要对自己言论负责)，网络空间中的监管是通过运用现代科技对网络用户发表的内容信息进行实质审查，不再是单纯的屏蔽涉及敏感词汇的内容，虽然对于打击网络犯罪有重要影响，但是会使所有人处于被全面监控的状态，几乎成为一个透明人。[5]公共空间也会存在很多私人活动，是存在个人隐私的，通过长期密集不间断的监控，又因为侦查对象的广泛性，会不可避免的扩大到第三人，无辜民众的信息也会成为侦查的对象，这对公众隐私权的侵害是直接、现实的，比如美国的“棱镜计划”，对网络用户存储的数据进行深度监控，其中难免损害不特定公众的个人信息安全，大规模监控将个人的行为记录等信息进行结合，就可以推测出被监控者不愿被人知晓的隐私信息，被监控者也通常并不知晓其个人信息已被监测、收集和使用等。

再者侦查机关对个人信息的过度收集使用也会加剧这一风险，由于侦破案件讲求证据，加上证据裁判主义的要求，[4]侦查机关通过大规模监控技术强制收集个人信息，难免会使信息主体对个人信息失去控制，并且收集信息时不加以区分个人信息的类型(敏感个人信息和普通个人信息)，敏感个人信息一旦泄露，会使公民权益造成更大的损害，不加区分的收集、使用个人信息，会使侦查机关成为个人信息的最大控制者，个人信息安全受到一定程度的侵害。

大规模监控与个人信息保护的冲突其实也可以说是公共安全保障与个人隐私保护之间的冲突，[6]对侦查中的大规模监控进行规范好像又回到了打击犯罪和人权保障这一原始命题上，在风险社会中，侦查机关进行大规模监控是为了更好的治理犯罪，保障公共安全，其中不可避免的遇到隐私保护问题，对大规模监控进行规制时需要进行利益衡量，注意比例原则的适用。

(二) 大规模监控和第三方数据

在信息社会，随着网络技术的发展，人们越来越依赖网络服务，个人通常将含有个人信息的言论发表在网络平台中，或者为了享受某种服务需要提交自己的信息，比如注册软件时进行的实名认证、获取的手机号码等，这些信息都会变成数据，在刑事诉讼中，大规模监控技术的使用使侦查方式发生了转变，侦查机关由信息的收集者变为使用者，为了防控风险、追诉犯罪的需要，往往依托于网络服务商所存储的各类信息进行侦查取证，那如此一来，网络空间存留的个人信息也会成为侦查中分析的对象，侦查机关收集这些个人数据是否会侵害个人的隐私权？是否是个人信息保护的对象？认为不侵犯隐私权、不属于个人信息保护对象的理由是：个人自愿将自己的信息提交至网络，就不具备对隐私的合理期待，会丧失合理的隐私权保护，这就是所谓的第三方理论，[7]信息主体一旦将个人信息在网络上公开，信息的私密性就不再，侦查机关利用这些信息不会侵害公民权利。但这一理论在信息化社会很难适用，因为当今个人为了参与现代生活的需要向第三方主体提供自己的个人信息是必要的，而且信息主体为了享受网络服务，将自己的个人信息向网络披露，是一种不得已的选择，比如对于手机 APP 的使用以同意隐私条款为前提，否则没有软件的使用权，这一同意行为客观上允许了第三方主体收集其个人信息，但如果不向网络服务商提交就会失去享受这种服务的权利，其实也可以说个人在一定程度上没有选择权，对于是否属于“自愿”行为是不好判断的，即使个人出于自愿将自己的个人信息提交给第三方，也并不会预见到后续侦查机关对其信息进行监控、收集和使用，这一侦查行为也超出了个人只是使用服务这一特定目的，所以不应认为个人信息因提供给第三方就失去了保护。对于侦查机关收集这些信息是否会对个人隐私权造成侵害，应根据不同情形分别考虑，如果侦查机关是事后收集，则不会侵权；如果是主动指令第三方收集这些个人数据，则会侵害公民隐私权。还有在大数据时代下，第三方数据除了包括内容信息，通常是以非内容形式存在的，大规模监控多数情况下也针对非内容性信息，比如通讯时间、交易地点等，通过对信息形式(非内容信息)要素的收集，再进行数据挖掘分析、结合其他碎片化信息进行比对，也可以描绘出一个人的完整图像，识别到具体的人，获知其人身、财产状况等生活细节全貌，威胁个人信息安全，

所以也不应认为非内容信息不属于个人信息保护的对象。

(三) 大规模监控与信息共享

这一问题侧重于对大规模监控事后挖掘信息的角度来说的，现在大数据时代下提倡信息共享，公安机关将通过大规模监控技术获取的信息在平台中共享，符合高效快捷的办事要求，但会存在个人信息泄露的风险，因为执法机关可能会对个人信息的使用不加约束。公检法信息共享平台很多都由内部系统管理，不对辩方开放，这会加剧控辩双方信息失衡的风险。[4]虽然辩方享有阅卷权，但是其适用范围在信息化时代下稍显狭窄，在这种情形下可以赋予辩方数据访问权，即有权从公检法机关获取其掌握的信息，来保障辩方平等了解案件事实信息和证据材料。

从目的原则来看，政府部门内部实行不同数据库之间的信息共享，但每个数据库信息的收集都是法律基于特定目的的授权，不同部门之间的数据共通、信息共享，也超出了原有的目的授权，违反了合目的性原则。[8]又比如大数据时代下，侦查机关对于信息的收集多从第三方机构获取，个人基于特定目的将信息授予第三方主体使用，执法机关基于追诉犯罪的目的使用第三方存储的信息，也已经超出了最初的授权目的。虽然政府部门之间实行数据共享，信息的使用超出了原有收集信息的特定目的，但总归都属于公共管理的范畴，与司法机关使用网络服务商管理存储的信息存在差异，对于此种情形的规则：原则上以查询为主，禁止复制拷贝其他部门数据库中存储的信息；建立全程留痕的回溯性技术监督程序等。

4. 个人信息保护与大规模监控的规制进路

侦查中运用大规模监控技术逃不开个人信息保护问题，对其规制从宏观层面和具体程序规制两个方面展开，并且要注意保护的限度。

(一) 宏观指导：遵循比例原则

对大规模监控进行规制原则上要实现犯罪治理、打击犯罪与人权保障之间的价值平衡，需要遵循比例原则进行宏观指导。个人信息保护中的比例原则，主要有目的和手段两个方面的规范，一是目的正当原则要求，具体是指在运用大规模监控技术收集个人信息时，遵循侦查、起诉、审判的目的，不能用于其他目的；[9]二是必要性原则和适当性原则，在侦查中监控个人信息应将把侵害个人信息的程度控制在最小范围内。

在手段方面，可以用场景化原理即针对不同主体对象、信息类型进行规制以平衡大规模监控与个人信息保护。第一，区分不同对象。对于针对特定对象的大规模监控事实上与刑诉法中的技术侦查相同，应该严格予以规制，因为在这种情形下，监控的一般都是针对特定案件诉讼主体的内容性信息，相比非内容性信息对个人信息的侵害更重；由于针对不特定第三人的大规模监控具有“面广但度轻”的特点，对个人信息入侵程度相对较浅，这种情况可以相对放宽。[3]第二，对不同的个人信息类型加以区分。基于比例原则，对敏感个人信息与普通个人信息分级管理，重点保护敏感个人信息，对敏感信息的收集设置更严格的启动条件(奉行最后手段原则)，比如对敏感个人信息的干预只能在立案之后侦查阶段进行，在预防阶段不能干预，调查阶段一般不能干预，但针对个案经过特殊程序许可的情形作为例外。

(二) 具体规制：权利保障和程序规制

1) 权利保障——知情权

关于知情同意原则在刑诉法的适用是否有必要也有一些争论，反对的理由通常是基于国家追诉犯罪的强制性、封闭性和秘密性等公共利益的维护上，认为这一原则没有适用的空间，但其实可以根据执法机关干预信息行为的强弱以及个人信息的重要性程度，实行分级保护制，对不同案件进行类型化区分。权利自然与义务相对应，要保障信息主体的知情权就需要司法机关的告知义务，比如在一般刑事案件中，同时为了追诉犯罪活动的顺利进行，在侦查工作基本完成或者结束后可以推迟告知而不用同步告知；在

危害国家安全犯罪、恐怖活动罪等重大犯罪案件中，如果告知可能威胁国家利益、泄露国家秘密等，可以作为告知义务的例外情形。以上的论述是基于特定对象来说的，如果是大规模监控下的非特定对象，信息主体如何知道其个人信息权受侵害也是一个问题，在侦查机关的告知对象不确定的前提下，告知义务又该怎样履行？所以对于不特定对象，由于大规模监控具有侵权面广但程度低的特点，侦查机关的告知成本又太大，知情同意原则没有适用空间。

2) 程序规则

从保护个人信息的角度对大规模监控进行规制，不管是前期的犯罪预防还是后面犯罪侦查功能，最终的目的都是为了追诉犯罪，所以从这一目的来看，应该将大规模监控纳入刑诉法的规制范围，加之其本身具有的强制性、秘密性，与技术侦查最为相似，可以适度扩大技术侦查的适用范围以便对大规模监控技术进行有效规制。[2]但我的技术侦查基本都是内部审核，缺乏外部监督，所以对大规模监控的规制应该注意这一问题，在内部控制的同时加强外部监督，可分为事前审批、事中监督和事后救济三部分。大规模监控的事前审批可以比照适用技术侦查措施的规定进行适用；在监控过程中，可以由检察机关对监控范围等进行监督，建立定期报告制度即公安机关定期向检察机关报告监控结果；事后救济指的是设置独立的个人信息保护部门或者信息监管部门，由于检察机关具有法律监督的职能，可以考虑在检察机关设置这一部门来专门负责信息安全工作。[10]

在信息社会的当下，随着大数据技术的发展，侦查人员在对犯罪事实和证据形成判断之前，往往就已经对数据进行了收集和分析，这也造成立案后滞于侦查的现象，不利于正当程序正当化的构建，大规模监控的即时性使得犯罪侦查和预防界限变得模糊，很难满足先立案后侦查的要求，以立案作为强制性的前提，不能保证突发犯罪时侦查的随时启动，建议结合侦查中的大规模监控运用现状，将立案改造成侦查阶段的前期工序。在侦查取证中，如果监控措施不合法，那侦查机关利用大规模监控收集的证据材料的合法性问题也会存在质疑，我国对于非法证据排除规则的规定限于言词证据、书证和物证形式，若从字面上理解，这一证据规则是不涵盖大规模监控收集的电子数据和视听资料的，所以建议将这两种证据也纳入这一证据规则中，但需要根据收集目的、适用对象、干预程度进行类型化区分。[3]

(三) 个人信息保护的限度

个人信息兼具个人利益和公共利益的属性，不能完全脱离公共利益，对其进行保护需要进行利益衡量。在大数据时代下更是如此，信息是宝贵的资源，是立案、侦查取证的重要线索，数据的价值往往就在于它的多次利用，对于制定针对性的公共政策，个性化的服务有很大帮助，所以在信息收集阶段赋予信息主体被遗忘权是否有必要？在大规模监控下，信息主体可能并不知晓其个人信息受侵害，没有机会行使这一权利，而且因为收集主体的多元化，又该向哪一主体寻求救济？从另一方面来说，赋予个人被遗忘权容易导致权利滥用，成本代价会很高，而且就算信息主体有机会行使这一权利，怎样保障已经公开的信息被别人遗忘，比如未成年人犯罪中有犯罪记录封存制度，但是由于新闻媒体的报道，别人是不会遗忘的，尤其是明星子女的信息泄露问题。“互联网是有记忆的”，网络空间的个人信息是难以被彻底遗忘的，被遗忘权的存在可能也是一个伪命题。个人信息保护需要有一定的限度，不能一味的强调限制监控技术和强化个体赋权来保障个人信息安全，会造成一定的信息障碍，而且也不符合大数据时代注重信息利用的要求，在数字时代背景下，对个人信息进行保护和使用需要并重，不能是绝对保护，而是有限度的保护。

5. 结语

公民基于现代化生活的需求，将个人信息让渡给司法机关以换取安宁和谐便捷的生活，将个人信息提交给网络运营商以换取某种服务，前提是需要司法机关、网络服务商能够正当使用公民的个人信息。

目前，刑事诉讼领域中的个人信息保护日益得到重视，伴随着大数据技术的快速发展，大规模监控虽然发挥着犯罪预防和侦查的作用，对侦查效率和精准度有所提高，适应了数字时代的需求，但这一技术的运用使得每个人处于被全面监控的状态，不可避免地引发一系列个人信息安全问题，应对其进行必要的规制，由于大规模监控的复杂性，需要从宏观和具体的程序设计上采取场景化原理、类型化区分的方法进行规制，虽然法律的发展往往落后于科技的发展，但任何制度设计都是从不成熟到成熟，相信随着对大规模监控技术研究的不断深入，能更好地保护个人信息安全。

参考文献

[1] 蒋勇. 大数据时代个人信息权在侦查程序中的导入[J]. 武汉大学学报(哲学社会科学版), 2019, 72(3): 156-164.

[2] 纵博. 侦查中运用大规模监控的法律规制[J]. 比较法研究, 2018(5): 82-105.

[3] 纵博. 隐私权视角下的大规模监控措施类型化及其规范[J]. 中国刑事法杂志, 2020(6): 55-71.

[4] 黎晓露. 个人信息权引入刑事诉讼的理论证成与体系化建构[J]. 河北法学, 2021, 39(12): 139-155.

[5] 刘艳红. 公共空间运用大规模监控的法理逻辑及限度——基于个人信息有序共享之视角[J]. 法学论坛, 2020, 35(2): 5-16.

[6] 郑曦. 刑事诉讼个人信息保护论纲[J]. 当代法学, 2021, 35(2): 115-124.

[7] 赵艳红. 大数据监控措施的法律规制研究——以隐私权为中心的探讨[J]. 交大法学, 2020(4): 132-148.

[8] 裴炜. 个人信息保护法与刑事司法的分离与融合[J]. 中国政法大学学报, 2020(5): 149-160+208.

[9] 程雷. 大数据背景下的秘密监控与公民个人信息保护[J]. 法学论坛, 2021, 36(3): 15-26.

[10] 于阳, 魏俊斌. 冲突与弥合: 大数据侦查监控模式下的个人信息保护[J]. 情报杂志, 2018, 37(12): 147-155.