**Dispute Settlement** 争议解决, 2023, 9(4), 1507-1515
Published Online July 2023 in Hans. https://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2023.94205

Hans汉斯

# 刑事诉讼中的个人信息保护

**钱素燕**

华东政法大学刑事法学院，上海

收稿日期：2023年5月29日；录用日期：2023年7月12日；发布日期：2023年7月21日

## 摘　要

**信息时代下刑事诉讼领域与其他领域一样存在保护个人信息的需要，然而目前我国相关法律规定零散且重视对公权力机关的授权忽视对公民的赋权。为确立和完善刑事诉讼个人信息保护机制，应根据目的正当、明确原则与比例原则、个人信息分级分类原则，对信息主体赋予知情权、数据访问权和数据更正、删除、限制处理权，对公权力机关(信息控制和处理者)科以告知义务、配合义务和数据安全保护义务。同时，通过建立多元化监督机制，设立专门的信息监管部门，构建侵犯信息权利的救济路径等，逐步建立起我国的刑事诉讼个人信息保护机制。**

## 关键词

**刑事诉讼，个人信息保护，规则构建**

# Protection of Personal Information in Criminal Procedures

**Suyan Qian**

School of Criminal Law, East China University of Political Science and Law, Shanghai

Received: May 29th, 2023; accepted: Jul. 12th, 2023; published: Jul. 21st, 2023

## Abstract

**In the information age, there also exists the need to protect personal information in the field of criminal procedure as in other fields. However, at present, the relevant laws in China are scattered and attach importance to the authorization of public authority while ignoring the empowerment of citizens. In order to establish and improve the mechanism of personal information protection in criminal procedures, information subjects shall be given the right to know, the right to access data, and the right to correct, delete, and restrict processing data following the principle of legitimate and clear purpose, the principle of proportion, and the principle of personal information classifi-**

文章引用: 钱素燕. 刑事诉讼中的个人信息保护[J]. 争议解决, 2023, 9(4): 1507-1515.
DOI: 10.12677/ds.2023.94205

**cation. Public authority (information controller and processor) shall be set up with the obligation of notification, cooperation, and data security protection. At the same time, through establishing diversified supervision mechanism, setting up special information supervision department, and constructing the relief path for violating information right, the personal information protection mechanism of criminal procedure in China can be gradually established.**

## Keywords

**Criminal Procedure, Protection of Personal Information, Construction of Rules and Regulations**



## 1. 问题的呈现

在历史的长河中，口耳相传的时代、书面与印刷传播时代已成为过去，人类已经进入了信息时代。在这个新时代，信息以前所未有的数量和速度进行传播，极大便利了人们的生活。但与此同时，人们的一言一行，无论在现实生活还是在虚拟世界里，都以信息的形式被监控、记录、存储、传输和使用；作为个体的人无力掌握自己的信息，如同困囿于“数字化圆形监狱”之中。为了摆脱此类困境，人们越来越重视个人信息的保护，许多国家或地区(尤其是欧盟)出台了大量关于个人信息保护的法律文件，最典型的即为欧盟《通用数据保护条例》(General Data Protection Regulation，以下简称“GDPR”) [1]。

在刑事诉讼中使用个人信息同样存在问题。其中，公民个人信息保护所面临的最大挑战，在于政府对公民个人信息进行的各类监控。在刑事司法、情报信息、国家安全三大领域，对公民个人信息的监控自古就有，但是，随着信息社会的深入发展，秘密监控与信息社会之间存在着相互融合、相互促进的关系。秘密监控已经成为获取和利用公民个人信息最广泛、最深刻的领域，尤其是随着大数据科技浪潮的兴起，公民在社会生活各个方面所留存的海量数据逐渐成为秘密监控的重要对象，以公民信息为载体的大数据也被应用到刑事司法、情报信息与国家安全等领域，公民信息被干预的规模与概率呈几何倍数的增长。

从个体的角度出发，以上所展现的刑事司法变革，实际上是一个“以隐私换安全”、“以信息换安全”的过程，公民让渡出部分个人信息由政府加以利用，从而获得更为安全、稳定的生活状态以及更为正当、更加文明的刑事诉讼程序，这种“交易”过程确属信息社会发展的必然。然而，交易存在对价，公民让渡个人信息权的前置条件是假定刑事诉讼程序能够正当化地利用公民个人信息[2]。因此，从法律层面上说，政府监控同样应通过正当程序加以规制。

刑事诉讼程序中的政府监控依赖于强大的信息资源和信息技术，对公民个人信息干预的广度、深度都远远超过公民个人、商业机构和社会机构，更为重要的是，政府对个人信息的使用本身就是一把“双刃剑”，一旦滥用，则将带来巨大的隐患。规制其对信息使用，不仅关系到信息社会的健康发展，更与公民的人格尊严、个人自治等一系列基本权利密切相关，显属法律规制的重点领域，理应加以认真研究、认真对待[3]。

## 2. 刑事诉讼个人信息保护立法现状及存在的问题

### 2.1. 国外规定概览

考虑到刑事诉讼中个人信息保护的现实需要，近年来，一些国家和地区采取了刑事诉讼中个人信息

保护的立法措施。根据《欧洲人权公约》第八条保护“私生活和家庭生活受到尊重的权利”的精神，2016年欧洲议会和欧盟理事会颁布了《关于保护自然人针对主管当局为预防、调查、侦破或检控刑事罪行或执行刑事刑罚而使用个人数据，和有关该数据的自由流动，以及撤销理事会第2008/977/JHA号架构决定的2016/680号指令》(以下简称为“欧盟2016/680号指令”)，较为系统地规定了刑事诉讼中个人信息保护的问题；2018年，《警察部门使用个人数据实务指南》出台，对警察部门执法中的个人信息保护问题进行规定。美国采用判例法的方式，通过2012年Jones案件[1]和2018年Carpenter案件[2]，以宪法第四修正案对公民隐私权的保护为路径，确立了政府对公民实施定位(包括GPS定位或手机定位)时的个人信息保护规则[4]。

## 2.2. 我国现行规定

我国暂不存在针对刑事诉讼中个人信息保护问题的专门立法。在《刑事诉讼法》中，直接涉及个人信息保护的内容只有第五十四条规定涉及个人隐私的证据应当保密[3]，第六十四条规定特定案件中公检法不公开证人、鉴定人、被害人个人信息[4]，第一百五十二条规定技术侦查中获悉的个人隐私应当保密[5]等。以刑事侦查为例，所谓强制性侦查措施，是指侦查机关在刑事侦查过程中采取的带有一定约束力并对公民权利造成一定限制的措施。大数据信息时代，社会需要从隐私权保护转变为个人信息权利保护已日益成为共识，大数据侦查中的数据收集、共享、挖掘等行为，涉及干预和限制公民的个人信息权利，也应包括在强制性侦查措施的范畴之内。根据程序法定原则的要求，强制性侦查措施的种类、适用范围、实施过程等均有必要以法律明确加以规定。与此相矛盾的是，由于现行《刑事诉讼法》预设的侦查情境并非基于信息时代的背景，大数据的收集、共享、挖掘等行为并未被单列为一种侦查措施，现有规定中存在三种侦查措施与大数据侦查具有较高关联度，分别为证据收集调取、勘验检查和技术侦查。然而，现行刑事诉讼法中对前述三种侦查措施的规定并未涵盖大数据侦查措施的种类和实施方式，相关司法解释和司法解释性质的文件也未能及时跟进侦查措施的动态变化，从而对其设定严格的批准及实施程序，进而导致大数据侦查与个人信息保护之间存在无法调和的冲突。

### 2.2.1. 收集和调取证据

《刑事诉讼法》证据章第五十四条第一款规定了证据收集和调取的行为[6]。站在刑事诉讼法理的角度上，该条文仅为涉及证据收集、调取的概括性条款，并非将其规定为基于特别授权条款的查封、搜查等侦查措施中的一种，因此，只能作为证据收集、调取的原则性规定，而无法成为严重干预公民个人信息权利的大数据侦查措施的法律授权依据。《公安机关办理刑事案件程序规定(2020年修正)》第六十二条[7]、六十三条[8]进一步规定了证据收集、调取行为的程序及对象，补充并细化了《刑事诉讼法》第五十四条。

[1]参见United States v. Jones, 565 U. S. 400 (2012).
[2]参见Carpenter v. United States, 138 S. Ct. 2206 (2018).
[3]《刑事诉讼法》第五十四条第三款：“对涉及国家秘密、商业秘密、个人隐私的证据，应当保密。”
[4]《刑事诉讼法》第六十四条：“对于危害国家安全犯罪、恐怖活动犯罪、黑社会性质的组织犯罪、毒品犯罪等案件，证人、鉴定人、被害人因在诉讼中作证，本人或者其近亲属的人身安全面临危险的，人民法院、人民检察院和公安机关应当采取以下一项或者多项保护措施：(一) 不公开真实姓名、住址和工作单位等个人信息；……”
[5]《刑事诉讼法》第一百五十二条第二款：“侦查人员对采取技术侦查措施过程中知悉的国家秘密、商业秘密和个人隐私，应当保密；对采取技术侦查措施获取的与案件无关的材料，必须及时销毁。”
[6]《刑事诉讼法》第五十四条第一款：“人民法院、人民检察院和公安机关有权向有关单位和个人收集、调取证据。有关单位和个人应当如实提供证据。”
[7]《公安机关办理刑事案件程序规定(2020年修正)》第六十二条：“公安机关向有关单位和个人调取证据，应当经办案部门负责人批准，开具调取证据通知书，明确调取的证据和提供时限。被调取单位及其经办人、持有证据的个人应当在通知书上盖章或者签名，拒绝盖章或者签名的，公安机关应当注明。必要时，应当采用录音录像方式固定证据内容及取证过程。”
[8]《公安机关办理刑事案件程序规定(2020年修正)》第六十三条：“公安机关接受或者依法调取的行政机关在行政执法和查办案件过程中收集的物证、书证、视听资料、电子数据、鉴定意见、勘验笔录、检查笔录等证据材料，经公安机关审查符合法定要求的，可以作为证据使用。”

从证据种类来看，大数据侦查证据收集、调取行为中的“证据”多为电子数据，与此相关的是2016年《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》(以下简称为《电子数据规定》)以及2019年《公安机关办理刑事案件电子数据取证规则》中有关“收集、提取电子数据”的规定。但是，其以“收集、提取电子数据”作为电子数据取证的基本概念和方法，规定了一系列电子数据的审查判断方式以及取证存证的具体实施规范，体现出将“收集、提取电子数据”作为独立于刑事诉讼法侦查章所规定的九种法定侦查措施的立规倾向[5]，其与《刑事诉讼法》中既有的侦查措施以及大数据侦查措施的关系尚待厘清。

#### 2.2.2. 勘验和检查

勘验、检查分为线下和线上两种形式。《刑事诉讼法》侦查章第四节“勘验、检查”仅规定了勘验、检查的线下模式，即以场所、物品、人身、尸体作为适用对象所进行的勘验、检查，并未涵盖该行为的线上模式，即对电子数据的勘验、检查行为。一般认为，大数据侦查中勘验、检查行为所针对的对象基本为电子数据，即《电子数据规定》第九条第三款规定的网络远程勘验[9]及第十六条规定的电子数据检查行为[10]。网络远程勘验与电子数据检查行为是“收集、提取电子数据”中的两种具体行为类型，相较于刑事诉讼法中规定的勘验、检查，其实施程序更加严格，增加了关于对电子数据存储介质拆封过程录音录像、制作电子数据备份等要求。该规定进一步证实了《电子数据规定》认可“收集、提取电子数据”这类行为的相对独立性，进而影响《电子数据规定》所载明的侦查行为与刑事诉讼法规定的侦查措施之间的有效衔接。

#### 2.2.3. 技术侦查

2012年《刑事诉讼法》修订时在侦查章新增了技术侦查措施一节，开启了技术侦查法治化的进程。技术侦查措施有力地回应了信息技术发展在刑事诉讼法领域的影响，但，基于其敏感性、隐蔽性与强烈的隐私侵入性，刑诉法对技术侦查措施的授权采用了模糊性质的做法，以回避的态度面对其内涵与外延的厘清，对启动条件的规定也较为模糊和笼统，技术侦查措施仅依据“根据侦查犯罪的需要、经过严格的批准手续”即可采取，不受最后手段原则的限制。在此基础上，《公安机关办理刑事案件程序规定》细化了有关技术侦查措施的实施主体、范围、批准手续等的规定。技术侦查措施属于典型的强制性侦查措施，与大数据侦查措施非常相似。就现有规定而言，大数据侦查措施和技术侦查措施是属种关系，大数据侦查措施为上位概念，其外延不仅包括以静态监控与调取为主的记录监控、行踪监控、通信监控、场所监控等措施，还更加侧重于对数据的动态建模挖掘与分析；在适用时间节点上既涵盖立案后的侦查阶段，也包括立案前的预警与调查核实阶段；在案件类型上除针对危害国家安全犯罪、恐怖主义犯罪等严重犯罪案件外，还针对电信网络诈骗、网络赌博等多发性犯罪案件。在实践中，大数据侦查技术已与多种技术侦查措施相结合进行使用，可见于《电子数据规定》第九条对网络远程勘验的规定，即在网络远程勘验过程中需要实施技术侦查措施的，必须依法经过严格的批准手续方可采取。然而，刑事诉讼法及配套规定中并没有详细说明哪些大数据侦查措施应当归属于技术侦查范畴，进而适用技术侦查措施的严格程序，导致侦查机关以采取的大数据侦查措施不属于技术侦查措施为由从而规避严格实施程序的现象较为常见[6]。

[9]《电子数据规定》第九条第三款：“为进一步查明有关情况，必要时，可以对远程计算机信息系统进行网络远程勘验。进行网络远程勘验，需要采取技术侦查措施的，应当依法经过严格的批准手续。”

[10]《电子数据规定》第十六条：“对扣押的原始存储介质或者提取的电子数据，可以通过恢复、破解、统计、关联、比对等方式进行检查。必要时，可以进行侦查实验。电子数据检查，应当对电子数据存储介质拆封过程进行录像，并将电子数据存储介质通过写保护设备接入到检查设备进行检查；有条件的，应当制作电子数据备份，对备份进行检查；无法使用写保护设备且无法制作备份的，应当注明原因，并对相关活动进行录像。电子数据检查应当制作笔录，注明检查方法、过程和结果，由有关人员签名或者盖章。进行侦查实验的，应当制作侦查实验笔录，注明侦查实验的条件、经过和结果，由参加实验的人员签名或者盖章。”

#### 2.2.4. 存在的问题

如前文所述，我国现行关于刑事诉讼中保护个人信息的规定主要存在两方面的问题。其一，零散而不成体系。相较于欧盟2016/680号指令的系统规定，我国无论是《刑事诉讼法》还是其他法律法规，涉及个人信息的规定散落于少数条文中，相关规定缺乏系统性，导致实践中执行不力、施行不畅。对于此，未来《刑事诉讼法》在修改时可考虑专设个人信息保护的章节，或者在个人信息保护的专门立法中设置专章规定刑事司法中的个人信息保护问题。其二，对公权力机关的授权多于对公民的赋权。上述涉及刑事诉讼的法律中有大量条款授权公权力机关收集使用公民个人信息，例如技术侦查制度、电子数据在线调取等，也含有公民或组织配合义务的规定，如《网络安全法》第二十八条中规定网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助[11]，但缺乏对刑事诉讼中公民个人信息权利的赋权性规定，使得以权利制约权力难以实现。

## 3. 刑事诉讼中个人信息保护的规则建构

### 3.1. 基本原则：保护权利与打击犯罪的利益平衡

刑事诉讼中的个人信息不仅承载着人格权益，而且具有证据价值。因此，刑事诉讼中保护个人信息的关键是积极履行个人信息的国家保护义务，限制公权力的不当行使。为实现法律起诉与个人信息保护的协调，应在目的正当原则和比例原则的指导下，建立个人信息保护的具体规则和制度。

根据个人信息保护法第四条规定，个人信息的认定必须符合三个条件：一是识别性，即根据对信息的分析能够识别或者确定某一个人；二是相关性，即信息应与个人相关；三是不属于匿名化处理后的信息。在刑事诉讼中，个人信息也须满足上述三个条件。从刑事诉讼打击犯罪、保障人权的目的，以及诉讼程序推进的阶段性切入，个人信息在不同诉讼阶段呈现不同的内容和特征。审前阶段中，案件相关人，如犯罪嫌疑人、被害人等的隐私信息、通讯信息、身份信息、家庭信息、行踪信息等，或者可证实犯罪嫌疑人有罪或无罪的案外人的个人信息，如侦查机关在犯罪嫌疑人排查时收集到的案外人的指纹、生物信息，都可以被划归为有助于破案的个人信息的范畴。审判和执行阶段中，诉讼参与人等的个人或隐私信息，特别是已被定罪罪犯、被判无罪者、线人等的信息，是这一阶段里个人信息的主要表现。为保障个人信息的安全性和私密性，防止因个人信息泄露而导致打击报复、恐吓、威胁等恶性行为，刑事诉讼通常选择不公开、保密或庭外核实的方式来处理个人信息。

从刑事诉讼强制性与特殊性的角度出发，既要充分梳理刑事诉讼内在的规律与特征来确立其中个人信息保护的规则建构；同时，也要充分考虑到打击犯罪与保护个人信息二者之间的平衡关系，适当调整私法领域中对个人信息保护的规定。据此，下述三个原则应予以遵循：

#### 3.1.1. 目的正当与明确原则

此原则的内涵下，专门机关若要对公民的个人信息进行收集与使用，必须要严格遵守法律的规定并取得有效授权，同时其行为需基于惩治犯罪的必要性，目的明确且具体，禁止将取得的个人信息应用于无关领域。例如，2021年10月6日，欧洲议会投票通过应全面禁止基于个人生物信息识别的大规模监控的决议，明确公民只有在涉嫌犯罪这一情况下才会被监控。专门机关若以惩治犯罪为由，需要收集、使用个人信息，也应明确并记录其目的。只有当专门机关出于明确和具体的目的收集和使用个人信息时，才能评估和监督专门机关是否存在过度收集或滥用信息的情况，从而降低人格尊严受到减损的风险。

#### 3.1.2. 比例原则

此原则作为限制政府公权力过多干涉公民私权利的重要原则，同样能在刑事诉讼的个人信息保护领

[11]《网络安全法》第二十八条：“网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。”

域中加以适用。更具体地来说，专门机关若想干预公民的个人信息，必须要判断其行为是否满足适当性原则、必要性原则以及狭义比例原则的要求。适当性原则的规定下，专门机关进行的干预行为需出于有利于惩治犯罪、侦破案件的目的。只有干预行为与目的相符合，才能满足此项原则的内涵。而必要性原则，则是对专门机关所采取手段的干预程度进行规制。在可以选择的情况下，优先适用对个人信息权利侵入性最低的方式。例如，尽可能降低对公民个人信息的影响性，严格把控收集信息的范围、授权的期限长度、留存的时间长短等。狭义比例原则，重点在于对专门机关不当干预个人信息的行为进行约束，强调干预公民个人信息的行为所带来的后续影响应当与此行为的进行所实现的目的程度相当，保证相对的平衡性。刑事诉讼中，干预目的正当、行为合乎比例，以此为基础，才能更好地处理依法追诉与保护个人信息之间的辩证关系。

#### 3.1.3. 个人信息分级分类原则

刑事诉讼涉及多元诉讼主体、信息种类繁多，且不同的权力行为对个人信息干预的内容和程度各异。若要实现对个人信息的有效保护，个人信息分级分类原则的确立刻不容缓。其一，个人信息内容不同，则适用的个人信息保护规则也应进行合理区分。通用情况下，就信息的保护程度而言，敏感个人信息大于一般个人信息，敏感隐私信息大于一般隐私信息，专门通信监控信息大于一般通信监控信息。比如说，基因和生物特征信息、行踪轨迹信息及未成年人前科记录等属于敏感个人信息的范畴，其保护程度理应更高、收集及使用程序理应更严格。只有在收集一般个人信息的情况下无法或难以有效打击犯罪，才能够进一步收集敏感个人信息。其二，公民个人身份不同，则适用的信息保护规则也应有所差异。刑事诉讼参与主体多元，享有权利与应尽义务不同，则不同主体对信息保护的要求也有区别。故，多元信息主体的信息保障措施与保护力度也不能一概而论。针对已被定罪罪犯，可根据案件性质、人身危险性等因素，梯度设置个人信息权利行使规则，如严格限制或剥夺性侵案件罪犯申请删除个人信息。对于经法定程序被判无罪者，在被判无罪后，原则上不应限制其个人信息权利的行使。对于遭受性侵的被害人，应重点保护其隐私信息[7]。

### 3.2. 具体构造：权利与义务的立法细分

“在我国强职权主义诉讼模式下，法律赋予公安司法机关收集使用个人信息的强大权力，以至于‘权利－权力’关系呈现出一种跛脚的状态[1]。”从“权利－权力”的视角切入，应当赋予公民个人信息权利。但值得注意的是，出于维护国家安全、社会公共利益的需要，引入个人信息权时需要为刑事司法“量体裁衣”，这就意味着应对个人信息权作必要限制。

#### 3.2.1. 信息主体的权利

刑事诉讼中的信息主体至少应当享有三类权利：1) 知情权。个人信息保护制度基于对相关主体知情权的尊重，《个人信息保护法》第七条规定：“处理个人信息应当遵循公开、透明原则，公开个人信息处理规则，明示处理的目的、方式和范围。”但是，刑事诉讼带有一部分的封闭色彩，这一特点在侦查过程中反映尤盛，因此对知情权加以合理限制是必要的。对此，有学者提出构建“告知－延迟告知－不告知”层级化制度[8]，比如说侦查机关可延迟至侦查工作结束后再向信息主体告知相关内容，尽最大可能调和知情权与刑事诉讼封闭性之间的矛盾。2) 数据访问权。数据访问权不仅是辩方了解控方证据的来源从而准备辩护思路与内容的前提，也是防止数据失真，并避免导致司法错误的必要基础。在信息层面，对辩护人的阅卷权进行升级是非常必要的，能够帮助辩方了解司法信息化的工作情况，实现从阅卷权向数据访问权的进阶。3) 数据更正、删除、限制处理权。这三项权利的目的在于限制公权力收集使用公民个人信息的行为。在信息主体发现办案机关掌握的与自己有关的信息是不正确或不完整的情况下，有权

要求办案机关加以核实并进行后续的更正、补充；当信息主体发现使用其个人信息的前提条件已不具备，如特定目的已消失或期限届满时，有权要求办案机关删除或者不公开相关信息；当个人信息的正确性、完整性处于不确定状态，或者该个人信息需要作为证据进行保全时，有权要求办案机关使用该信息的前提为取得了信息主体的同意。

#### 3.2.2. 信息处理者的义务

公安司法机关出于刑事诉讼的目的而收集使用个人信息，其身份定位于信息处理者，有义务承担相应的责任。具体地说，首先是与信息主体权利对应的义务，主要包括通知义务与配合义务。通知义务与信息主体的知情权对应，通知的内容应包括收集使用公民个人信息的目的、对应法律依据以及相关的救济途径。配合义务指的是“信息处理者应配合信息主体行使权利”[9]。例如，针对数据访问权，提供访问权限和数据副本；针对更正权，更正不准确的信息、补充不完整的信息；针对被遗忘权，删除或封存已失去诉讼使用目的的信息。其次是数据安全保护义务。依据《数据安全法》第四章“数据安全保护义务”第二十七条规定，公安司法机关应当“建立健全流程数据安全管理制度，采取相应的技术措施或其他必要措施保障个人信息安全[12]。”主要包括：对个人信息(尤其是是敏感信息)严格履行保密义务，确保采取了必要的技术措施以保证信息处理的安全性；对个人信息的处理过程进行全阶段的记录，建立操作日志与操作留痕机制；在收集使用个人信息时，比对合目的性和比例性的要求，评估该行为对公民隐私、财产和人身安全带来的风险；一旦有泄漏信息的情况发生，及时向主管部门报告并通知信息主体，尽可能快速地采取补救措施，降低事故的影响[10]。

### 3.3. 权利保障：监督与救济途径的有效构建

“无救济则无权利”。为了有效保护公民在刑事诉讼中的个人信息权，需要构建对应的监督与救济途径，主要包括建立多元化监督机制、设立专门信息监管部门和构建权利救济路径三个方面。

#### 3.3.1. 建立多元化监督机制

根据干预的强度，可以将对个人信息的收集与处理行为作出内部自控与司法审查的界分。例如，针对特定的犯罪嫌疑人所实施的以侦查为目的的信息收集行为，可以按照其干预程度的强与弱区分成强制侦查以及任意侦查，相对应地分别采取内部自控与司法审查的方式。我国目前涉及个人信息的侦查措施(包括技术侦查)主要是内部自控，但是，从现代监督制约权力的理念上看，此种内部自控的方式在面对部门利益时，存在一定的局限性，尤其是审查工作难以真正发挥有效的作用。如此，这样的现象便为构建司法审查机制创造了制度上的契机。比如，美国将符合隐私期待“主客观双重判断标准”的电子数据取证行为认定为“搜查”，只有在司法官签发司法令状的前提下才能实施。因此，在对个人信息的收集处理行为进行类型化区分的基础之上，综合运用内部审批与司法审查的方式来推动程序正当化是更为合理的。

#### 3.3.2. 设立专门的信息监管部门

为了有效监督权力机关处理个人信息的行为，国家可以根据现实的需要设置专门的信息监管部门。如 GDPR 已将欧盟个人数据保护委员会设立为最高监督机构，并要求成员国成立数据保护监督机构。德国《联邦个人资料保护法》规定了“个人资料保护监察人”制度，监察人既负责受理公民对权力机关收集处理个人资料时侵犯了其权利的申诉，还可以向其提出改正建议。此类制度在我国也拥有相似的规范基础。《个人信息保护法》第六十条规定：“国家网信部门负责统筹协调个人信息保护工作和相关监督

[12]《数据安全法》第二十七条：“开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。”

管理工作。”但是，国家网信部门监管的范围涵盖全社会，难以准确把握刑事司法的特殊性。基于检察机关法律监督者的宪法地位，可以考虑在检察机关内设信息监管部门，专门性地负责刑事司法活动中的信息安全监督工作，同时履行司法审查职责。

#### 3.3.3. 构建权利救济路径

《个人信息保护法》第六十一条规定，公民有权向履行个人信息保护职责的部门投诉、举报[13]；《刑事诉讼法》第五十六条[14]、五十七条规定了针对非法取证行为的制裁措施[15]。基于上述规定，可以从三个方面构建刑事诉讼中的个人信息权利救济路径：第一，对于情节相对轻微的侵犯公民个人信息权的职务行为，相关机构按照公民的投诉内容进行调查，核实情况后对责任人员处以纪律惩戒或行政处罚；若情节严重构成犯罪，则移送司法部门以追究刑事责任。第二，侵犯公民个人信息权的行为一旦满足了《刑事诉讼法》第五十六条规定的“不符合法定程序”“可能严重影响司法公正”“不能补正或者作出合理解释”情形之一的，权利主体有权申请非法证据排除，检察机关有义务审查取证行为是否合法，若情节严重，相应证据应当予以排除。第三，如果公民的人身权与财产权因刑事诉讼中收集使用个人信息的行为而遭受损害，那么实施侵权行为的办案主体应当承担赔偿责任。

## 4. 结语

在本文结尾，回顾审视文章开头提出的“以信息换安全”这一命题仍然具有必要性。信息社会的本质要素即为信息，其流动与共享驱动了全社会的发展。在这样的社会发展形态当中，作为社会控制机制之一的刑事司法系统必然需要发展各类秘密监控手段与能力，公民个人通过让渡部分的信息权享受了信息社会带来的便利与发展成果，包括更为和平、安全、和谐的社会大环境。从这个角度上来说，“以信息换安全”是信息社会发展的必然。另一方面，“用信息换安全”的价值权衡过程也与其他交易过程类似，其与风险并存，都得面临衡量与取舍。除了追求安全价值，人类的发展离不开追求人格尊严与个人自治等更高阶的价值目标，而信息社会之中，保障公民的个人信息权就是实现人格尊严、个人自治等价值的必要前提。因此，公民让渡出部分个人信息后，必须要配备一系列健全且严密的制度设计才能够保障政府以合法、合理的方式使用个人信息。古往今来，滥用信息所造成的严重后果数不胜数。除了本文提出的相关建议之外，紧随信息技术的快速发展并加以持续探索，不断回应技术创新所引发的规制难题仍具有现实必要性，如此才能真正实现“用信息换安全”。

## 参考文献

[1] 郑曦. 作为刑事诉讼权利的个人信息权[J]. 政法论坛, 2020, 38(5): 133-144.

[2] 郭锐, 缪因知. 绿竹猗猗——安守廉教授与中国法学界交流纪念文集[M]. 北京: 中国人民大学出版社, 2019.

[3] 程雷. 刑事司法中的公民个人信息保护[J]. 中国人民大学学报, 2019, 33(1): 104-113.

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

[5] 龙宗智. 寻求有效取证与保证权利的平衡——评“两高一部”电子数据证据规定[J]. 法学, 2016(11): 7-14.

[13]《个人信息保护法》第六十一条：“履行个人信息保护职责的部门履行下列个人信息保护职责：(一) 开展个人信息保护宣传教育，指导、监督个人信息处理者开展个人信息保护工作；(二) 接受、处理与个人信息保护有关的投诉、举报；(三) 组织对应用程序等个人信息保护情况进行测评，并公布测评结果；(四) 调查、处理违法个人信息处理活动；(五) 法律、行政法规规定的其他职责。”

[14]《刑事诉讼法》第五十六条：“采用刑讯逼供等非法方法收集的犯罪嫌疑人、被告人供述和采用暴力、威胁等非法方法收集的证人证言、被害人陈述，应当予以排除。收集物证、书证不符合法定程序，可能严重影响司法公正的，应当予以补正或者作出合理解释；不能补正或者作出合理解释的，对该证据应当予以排除。在侦查、审查起诉、审判时发现有应当排除的证据的，应当依法予以排除，不得作为起诉意见、起诉决定和判决的依据。”

[15]《刑事诉讼法》第五十七条：“人民检察院接到报案、控告、举报或者发现侦查人员以非法方法收集证据的，应当进行调查核实。对于确有以非法方法收集证据情形的，应当提出纠正意见；构成犯罪的，依法追究刑事责任。”

[6] 刘玫, 陈雨楠. 从冲突到融入: 刑事侦查中公民个人信息保护的规则建构[J]. 法治研究, 2021(5): 34-45.
[7] 李艳飞. 刑事诉讼中个人信息保护应遵循四原则[N]. 检察日报, 2021-12-01(003).
[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] 郭北南. 个人信息的民事法保护与救济[J]. 国家检察官学院学报, 2021, 29(2): 151-161.
[10] 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.