Advances in Social Sciences 社会科学前沿, 2023, 12(7), 4115-4123
Published Online July 2023 in Hans. https://www.hanspub.org/journal/ass
https://doi.org/10.12677/ass.2023.127561

Hans汉斯

数字化时代下公民个人信息保护的挑战与应对

马　燕

华东政法大学经济法学院，上海

收稿日期：2023年5月20日；录用日期：2023年7月21日；发布日期：2023年7月31日

摘　要

个人信息保护涉及国家安全和公民个人权益，理应予以重视。在此基础上，本文梳理了我国关于个人信息保护的法律规定，发现当前个人信息保护存在如下问题：部门授权路径不可控；概念界定不清晰；模糊性治理下的政府权力无序扩张；“知情同意”原则空置。针对上述困境，提出以下应对策略：细化知情告知原则；严格规定个人信息识别的收集处理流程；坚持个人信息识别收集中的比例原则。

关键词

个人信息保护，知情同意，个人信息识别，比例原则，技术应用范围

Challenges and Responses to the Protection of Citizens' Personal Information in the Digital Age

Yan Ma

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

Received: May 20th, 2023; accepted: Jul. 21st, 2023; published: Jul. 31st, 2023

Abstract

The protection of personal information involves national security and the rights and interests of citizens, and should be taken seriously. On this basis, this paper compares the legal provisions on personal information protection in China and finds that the following problems exist in the protection of personal information: the uncontrollable path of departmental authorization; unclear definition of concepts; disorderly expansion of government power under ambiguous governance; and the vacancy of the “informed consent” principle. In response to the above dilemmas, the following strategies are proposed: refining the principle of informed consent; strictly regulating the

文章引用: 马燕. 数字化时代下公民个人信息保护的挑战与应对[J]. 社会科学前沿, 2023, 12(7): 4115-4123.
DOI: 10.12677/ass.2023.127561

collection and processing process of personal information identification; and adhering to the principle of proportionality in the collection of personal information identification.

Keywords

Protection of Personal Information, Informed Consent, Identification of Personal Information, Principle of Proportionality, Scope of Application of Technology Format

Copyright © 2023 by author(s) and Hans Publishers Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/
Open Access

1. 引言

自 2004 年政府信息第一案公开以来，公民个人信息保护逐步引起重视。但随着数字社会的建设与发展，大数据、云计算、人工智能等技术创新公民个人数据信息安全正受到全方位挑战，公民的个人信息逐渐被“数字化”，随之带来的即是公民个人信息的“可隐性”的逐步瓦解，隐私的成立和维护变得岌岌可危[1]。事实上，公民个人信息被违规收集早已不是个案现象，而是在各行各业普遍存在，近年来我国不同部门针对侵害个人信息的行为都给予了严厉的打击，私人侵害个人信息的行为也得到了有效遏制，政府对公民个人信息的处理管控也更加严密。

2020 年新型冠状病毒肺炎全面爆发，包括中国在内的世界各国都遭受了极大的冲击。为了进行疫情防控，我国各级政府利用新型技术、大数据平台将互联网终端收集得到的公民的信息数据化。通过对公民信息数据的有效整合，以求知晓个体健康状况，进而精准定位。如发现异常，则可利用大数据，快速调出数据，查找当事人身份信息、住址，以求在疫情扩散之前即对当事人进行防控。地方政府部门也以相关数据为基础，以省、市、县、乡(镇)街道及各单位为依托，将个人信息数据转化利用，进而推出了健康码、每日打卡等制度，实现了个人信息的二次利用，个人信息数据化让“数据多跑路，公民少跑路”的模式得以成型，使得制度路径层面上遏制了人传人的可能，可见严格的防控措施在疫情初期无疑对遏制疫情蔓延产生了极大的作用。

2023 年 2 月 23 日，国家卫健委宣布我国取得疫情防控重大决定性胜利，本轮疫情已基本结束[2]。我国有关新冠疫情的防控也应由超常规向常态化转变。在欣喜疫情防控取得决定性胜利的同时，疫情中一些“超常规”的“有效”手段带来的侵犯个人信息的问题却值得在今后的法律体系建设中予以弥补。在此次新冠疫情中，当新冠肺炎被确定具有“人传染人”的特性，且有致死之可能后，普通民众感受到了来自不可控因素对自身生命的威胁，在这一阶段个人的力量显得十分有限，为了自身的生命权、健康权，需要政府扩张权力进行宏观调控。正如博登海默在《法理学》中所提及的，社会成员的私人利益有时与公共利益产生冲突，甚至侵害和危及公共利益[3]。在这一特殊背景下，政府为保护公共利益而对社会管理进行全面调控，其正当性不言而喻。但与此同时个人数据泄露的风险也大大提高，例如在此次新冠病毒肺炎疫情全面爆发后不久，有超过 7000 名武汉、湖北返乡者的个人信息被大肆泄露[4]；2020 年 1 月 28 日在湖南省益阳市赫山区，也出现了卫生健康局有关工作人员将属于内部工作文件且涉及多人隐私的调查报告转发给无关人员，造成严重社会影响[5]。可见，在二十大开局之年中，如何有效保护个人信息，规范政府，让政府依法行政，使“因事而扩张”的公民个人信息收集权力实现“克减”已然要提上日程。

2. 个人信息保护中存在的问题

2.1. 部门授权路径不可控

作为特殊的信息收集处理者，行政机构承担着提供公共服务、维护社会治安的重要职责。因此在公共领域内基于对公共利益的追求，进行个人信息的收集、处理具有其合法性和必要性。例如新冠疫情期间的大数据排查工作、追捕逃犯、进行出入境管理的边防安检工作等。

但因为有关行政机构收集、处理信息的法律法规和相应的监督机制尚不完善，行政机构收集个人信息的目的、范围、储存期限以及发生违法收集、信息泄露等情形时的救济方案都存在着模糊之处。这难免使人们产生对个人信息泄露的担忧。根据个人信息保护相关现行法律法规(见表 1)，基本下至街道、村，上至部委，皆有可能得到授权，而该部门是否真正得到授权公民几乎无处求证。作为政府各级行政部门下达的收集信息的指令而言，普通民众客观上是无法探寻其行政指令是否合理，公民面对这一局面做出抗争性质疑的难度较大，往往采取阻抗性、消极投入的方式，渐渐形成社会冲突，呈现出在社会互赖理论建构下的疫情防控个人信息保护冲突脉络(见图 1)。值得注意的是，立法者似乎也注意到了这一问题。在前文所列的《中华人民共和国个人信息保护法》中条款加入“紧急条款”这一限定语，“紧急情况”，这就要求我们在实施这一条款时要满足紧急事件的两大特点，即事态演变的高度不确定性和严重危害性[6]。

Table 1. Summary of current laws and regulations relating to the protection of personal information
表 1. 个人信息保护相关现行法律法规简略表

序号	法律法规名称	相关条款	说明对象
1	《传染病防治法》	第十八条第一款规定：“各级疾病预防控制机构在传染病预防控制中履行下列职责：……(二)收集、分析和报告传染病监测信息，预测传染病的发生、流行趋势；……”；第二十条第一条第二款规定：“县级以上地方人民政府应当制定传染病预防、控制预案，报上一级人民政府备案。传染病预防、控制预案应当包括以下主要内容：……(二)传染病的监测、信息收集、分析、报告、通报制度；……。”	① 各级疾病预防控制机构享有信息收集权。② 县级以上人民政府有权制定疫情防控的信息收集制度。
2	《突发事件应对法》	第三十七条第二款规定：“县级以上地方各级人民政府应当建立统一的突发事件信息系统……”；第三十八条第一款规定：“县级以上人民政府及其有关部门应当通过多种途径收集突发事件信息。”	明确了县级以上人民政府及其有关部门在疫情防控过程中建立信息系统并收集信息的职责。
3	《突发公共卫生事件应急条例》	第四十条规定：“传染病暴发、流行时，街道、乡镇以及居民委员会、村民委员会应当组织力量，团结协作，群防群治，协助卫生行政主管部门和其他有关部门、医疗卫生机构做好疫情信息的收集和报告、人员的分散隔离、公共卫生措施的落实工作，向居民、村民宣传传染病防治的相关知识。”	授予街道、乡镇以及居民委员会、村民委员会协助有关部门采集信息的权限。
4	《关于做好个人信息保护利用大数据支撑联防联控工作的通知》	除国务院卫生健康部门依据《中华人民共和国网络安全法》《中华人民共和国传染病防治法》《突发公共卫生事件应急条例》授权的机构外，其他任何单位和个人不得以疫情防控、疾病防治为由，未经被收集者同意收集使用个人信息。	除授权机构外任何机构无权收集

Continued

5	《中华人民共和国刑法》	第 330 条规定拒绝执行县级以上人民政府、疾病预防控制机构依照《传染病防治法》提出的预防、控制措施的，即涉嫌妨害传染病防治罪。	公权力介入
6	《中华人民共和国个人信息保护法》	紧急情况下为保护自然人的生命健康和财产安全无法及时向个人告知的，个人信息处理者应当在紧急情况消除后予以告知。	明确界定“紧急状态”

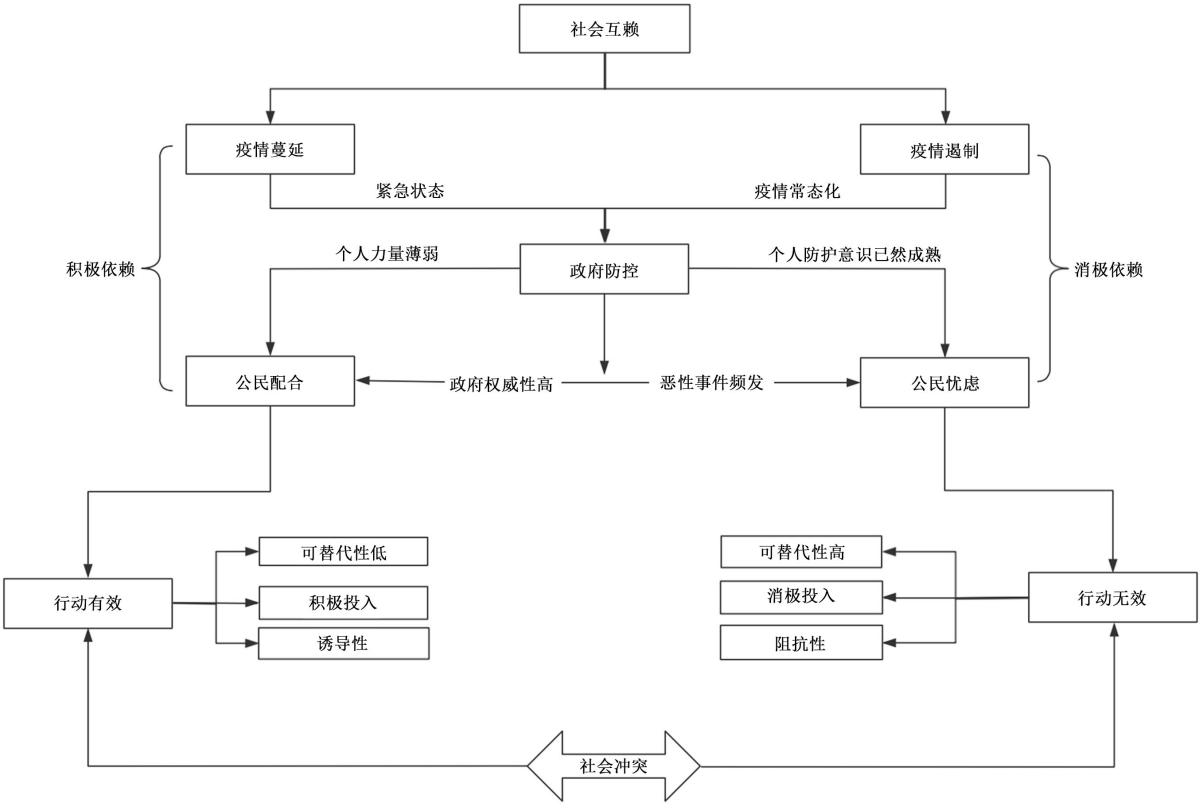

Figure 1. Context of social interdependence theory
图 1. 社会互赖理论脉络

2.2. 概念界定不清晰

我国对个人信息的研究始于上世纪 90 年代。随着大数据时代的到来，公民个人信息的商业价值日益显现。研究个人信息如何保护，那我们首先要界定何为个人信息。个人信息在理论界有三种不同称谓：个人隐私、个人数据、个人信息。对于这三种关系学界当前莫衷一是[7]。就民法角度而言，有学者认为个人信息是指与特定个体相关联，能够识别特定个人的文字、符号、图像、视频、音频等资料，它涉及个人身份、工作、教育、社交、财产等多维度的内容[8]。根据 2017 年两高颁布的司法解释以及 2020 年颁布的《民法典》中对个人信息可作以下界定，即通过电子或其他方式对不特定公民的个人信息可进行无障碍的记录与识别。就行政法视角而言，就疫情初期政府收集公民个人信息的行为，《中华人民共和国个人信息保护法》第十九条指出个人信息处理者处理个人信息，有法律、行政法规规定应当保密或者不需要告知的情形的，可以不向个人告知前条规定的事项中明确写明：紧急情况下为保护自然人的生命

健康和财产安全无法及时向个人告知的，个人信息处理者应当在紧急情况消除后予以告知。这一条文已表明新冠肺炎疫情发生以来，有关部门和地方依托大数据等新技术推出“行程卡”、“健康码”等应用程序，收集汇总疫情防控相关个人信息属于处理个人信息的合法情形之一。这一草案无疑为政府部门收集信息的合法性做好铺垫。当前学界主流观点认为国家权力是解决当前信息行业乱象丛生，维护国家和社会公共利益的关键，越来越多的学者呼吁将个人信息保护纳入公益诉讼办案范围[9] [10] [11] [12]。从刑法视角而言，当前学界主要有个人信息权说、个人人格权说、网络隐私权说、集体法益说、公共信息安全说等代表性观点[13]。这些观点基本可归纳个人信息的基本特征：私密性、专有性[14]。综上所述，本文在此给个人信息及个人信息非常态化收集条件做出如下定义：即个人信息是指与特定个体相关联，能够识别特定个人的文字、符号、图像、视频、音频等资料，具有一定的私密性、专有性。个人信息非常态化收集条件即《中华人民共和国个人信息保护法》所规定之：紧急情况下为保护自然人的生命健康和财产安全无法及时向个人告知的，个人信息处理者应当在紧急情况消除后予以告知。

2.3. 模糊性治理下的政府权力无序扩张

随着全面深化改革的逐步推进，中央在布置任务时越来越多地选用任务目标不明确或具有多重解释的模糊性任务，由此现阶段作为具体执行任务的地方各级政府，在任务完成过程中执行的模糊性程度不断提高[15]。由此模糊式治理愈来愈成为地方政府治理模式的体现之一，很多需要整体性布局的工作也越来越多地以模糊性任务的形式布置。关于模糊性治理，法学、管理学和政治学等多个学科都有涉及，模糊性的含义也包含多个层面，法学视角强调规则与规则执行的模糊性[16]。就我国而言，无论是从历史发展背景、阶段，还是现有社会政治经济制度、文化底蕴等都决定了我国政府处于强势地位。这种强势既是自西周以来家国一体的政治传统的传承，又是到如今“举国体制”的需要和政治保障[17]。积极而强势的政府也就不足为奇了，由此作为政府则具有积极的能动性、全面动员的合法性等相关特征[18]。面对新冠疫情这样特殊的重大危机事件，政府采取强有力的措施尽最大可能维护国家整体安全是应有之义。作为防疫工作的重要内容之一，对公民个人信息的收集有其必要性和合法性。但同时，模糊性治理也给地方行政机构留下了较多的自由裁量空间，由于缺乏相关法律规定和行政法规的明确指引，使得行政机构在具体场景中应用个人信息时，往往缺乏必要性审查和相应的风险评估环节，而只冠之以“维护公共利益”、“履行法定职责”的名号，因而在实际执行过程中如何避免以维护公共利益之名任意收集、处理公民个人信息，如何平衡社会公共利益与公民合法权益是模糊性治理所面临的重要问题。

2.4. “知情同意”原则空置

知情同意原则起源于18世纪普通法系中医事相关法律，强调医生应当在手术前告知患者相关的风险和结果，并在获得患者的同意后再进行手术，构成“告知－知情－同意”的基本原则[19]。在长期演变过程中，知情同意原则又在各国经历了不同的本土化发展。如2018年欧盟颁布的GDPR中，在确立知情同意原则作为收集处理个人信息的一般原则的基础之上，还明确规定了其他几种收集处理个人信息的豁免情形，即履行合同所必需、履行法定义务、保护信息主体或其他自然人利益所必须、维护公共利益以及处理者、第三方主体追求正当利益；同时，规定信息主体有权随时撤回同意，在撤回之前基于同意做出的个人信息的收集、处理的合法性不受影响[20]。GDPR中的这些规定，实质是在传统知情同意原则的基础上进行了完善，增添了关于知情同意的撤回、知情同意例外情形的相关规定。我国的相关法律中也有对“知情同意”原则的相关规定，并在立法规范中得到了反复确认[21]。但在实践中却面临着知情同意原则流于形式化和概念化、长期空置的尴尬局面。

首先，从立法规定角度来看，尽管个人信息保护的相关法律中都或多或少涉及到“知情同意”原则，

但却没有一部法律对知情同意原则的各个环节如何落实做出规范，即信息处理者应当采取何种方式、以何种语言表达方式告知信息主体哪些方面的事项？在个人知识程度存在较大差异的前提下，如何确保个人信息主体的充分知情？个人信息主体的同意应当以何种方式做出？不同类别的个人信息是否可以采取不同的同意表示方式？信息处理者在多次处理同一信息主体的个人信息时是否应当在每次处理前都征得个人信息主体的知情同意？即使《信息安全技术个人信息安全规范》中有涉及“明示同意”的明确规定，但却由于标准规范本身的效力等级较低，发挥的实际指导作用有限。

其次，从信息主体和信息处理者的角度来看，知情同意原则的某些规定并不适应大数据时代的发展需求。大数据时代信息处理者对信息主体的知情告知一般是通过各类隐私条款和用户协议，这类协议大多十分冗长，且含有一定量的专业术语。大部分用户由于时间和专业性有限，都不能做到通篇仔细阅读和理解。即使有用户耐心阅读了相关告知内容，由于信息处理者采取“用户不进行知情同意，就无法使用相关服务”的模式，用户实际上也不具备做出“知情但不同意”表示的可能性。而从信息处理者的角度来看，特别是在公共场所应用人脸识别技术，在同一时间可以捕获到海量的人脸识别信息，在对人脸识别的信息收集之前逐个征求信息主体的知情同意同样也是不现实的[22]。

再者，从个人信息收集处理的过程来看，信息处理者收集到的个人信息常常会经历多次的处理和分析，还会在不同信息处理主体之间进行多次流动。知情同意原则在初次收集环节尚可实现，但在后续的个人信息传播和多次处理环节，就存在着高昂的经济成本和较大的现实困难。强制在个人信息收集处理的各个环节征求知情同意也不利于个人信息的合法自由流动，不利于大数据相关产业的良性发展[23]。因此，信息处理者在实践中往往采取一揽子的“打包式”知情同意模式，用户只要点击“同意”，信息处理者就可以获得用户多种个人信息在收集处理全过程中的知情同意，这加剧了信息主体与信息处理者之间的不平等地位。

3. 数字化时代下公民个人信息保护的应对之策

法律规定的模糊性给行政机构应用个人信息识别技术留下了较多的自由裁量空间。由于缺乏相关法律规定和行政法规的指引，行政机构在具体场景中缺乏必要性审查和相应的风险评估环节，带来绕过个人信息主体的知情同意环节，冠之以“维护公共利益”、“履行法定职责”的名号的问题。这些立法工作上的模糊地带，应当通过法律加以完善。

3.1. 细化知情告知原则

3.1.1. 进行充分告知

充分、全面、准确的信息是个人信息主体做出科学决策的前提，信息不透明、未进行充分告知，则不构成“知情”。要充分保障其信息自主权，首先要保障个人信息的收集处理者在收集、处理前对相关事项进行了充分的告知，并且基于个人信息主体的认识能力，达到对于个人信息处理全过程的相关事项和可能带来的风险后果有了全面、清晰、准确的理解。在这一点上，可以参考欧盟 GDPR 中关于“信息透明度义务”的相关规定，即信息处理者应当以简洁、透明、易懂、易于访问的形式提供数据收集者、收据保护人员、数据处理目的和法律依据、存储期限、个人信息主体享有的相关权利以及信息处理的可能后果等相关信息。对于无民事行为能力人和限制民事行为能力人，则要对其监护人进行充分告知，获得其监护人的知情同意。考虑到大数据算法在处理个人信息过程中的不确定性，要求信息处理者在 一开始就告信息收集处理的全部内容存在着现实上的困难。因此，对于充分告知的信息应当限定在一般此类信息收集、处理中囊括的相关事项范围之内。由于充分告知条款中不可避免地存在着一些专业术语和复杂概念，建议相关行业组织出台相关术语标准，规范同一行业内知情告知条款中词句的运用，便于用户

理解和掌握。

3.1.2. 信息构建“动态同意”模式

动态同意模式，指的是允许个人选择其偏好的知情方式、频率及内容，并自由决定授权同意或退出同意[24]。由于个人信息识别技术应用过程中的不确定性、个人信息识别收集处理过程的反复性，信息主体难以在一开始就做出符合预期的知情同意，在获得信息主体的知情同意时，“初始同意即全过程同意”模式难以充分保障敏感个人信息的安全性。因此，有必要在引入“动态同意”模式，考虑信息主体在不同情境下的合理预期。动态同意模式具有下列特点和优势：第一，在动态同意模式下，个人可以根据偏好选择合适的告知时间、形式和内容，充分参与到告知环节中；第二，信息主体可以更为便捷地行使同意撤回权，有权依据人脸识别信息处理目的、应用场景、处理过程的变化情况，选择是否继续予以知情同意或者选择撤回同意。以疫情防控期间小区采取人脸识别技术识别进出人员身份、获得的人脸识别信息为例，若后续人脸识别信息的处理目的从疫情防控变为日常门禁管理时，业主就有权撤回其的知情同意，要求删除在进出小区时留下的人脸识别信息；第三，通过搭建相应的信息平台，信息主体可以实时了解到个人信息处理流程和进度，打破以往个人信息收集处理阶段的“黑箱”局面，提高信息处理的透明度[25]。

3.1.3. 细化同意类型

动态同意模式虽然在保障个人信息主体的信息自主权、提高信息处理的透明度和安全性上有着突出优势，但也因为进行多次知情同意以及撤回同意带来了信息收集处理的低效率、高昂的经济成本和时间成本等问题。因此在实践中，需要将动态同意模式与其他同意模式结合使用，并依据不同场景下人脸识别信息的收集目的、处理方式等信息，选择最为恰当的同意模式。个人信息属于敏感信息，一旦被非法收集或处理，将会给信息主体的信息安全、隐私保护、财产带来难以挽回的损失，应当采用更为严格的知情同意标准。因此除了法律法规规定的例外情形，在一般情况下获得信息主体的知情同意应当限定为明示同意类型，排除默示同意、推定同意的运用，以充分保障信息主体的知情权和选择权。在明示同意下，又可以将同意细分为特别同意、概括同意、动态同意等类型。特别同意即要尽可能全面地将一切相关信息和处理信息的可能风险后果告知给个人信息主体，此模式下个人信息主体的知情权和信息自主权可以得到充分的保护和尊重，对于信息处理者则施加了较为严格的告知义务；概括同意强调信息主体在授予知情同意时，其同意范围是一个做出宽泛限定的大概框架，信息处理者在此框架内进行信息收集处理则无需再获得知情同意。概括同意能够有效降低反复获得信息主体知情同意的成本，提高信息收集、处理的效率，但同样面临着对于信息主体隐私保护不到位、信息泄露的质疑。此外，还有大量在特别同意与概括同意之外的探索，如排除条款同意、分类分层同意、分阶段同意等[26]。不同同类的同意模式各自有其优势和缺点，应当结合使用，以构建科学合理的同意层级。

3.2. 严格规定个人信息识别的收集处理流程

在行政机构进行人脸识别信息的收集处理之前，首先应采取必要的技术措施或邀请具有相关资质的第三方机构，进行风险评估，分析在具体场景下收集个人识别信息的必要性、效率性和安全性。其次，应当通过草案公示、听证会、网络问政等多种渠道进行信息公开，将收集处理个人信息的必要性、识别信息的处理流程、采取的安全措施、信息储存期限以及可能带来的风险情况对公民进行充分告知。在此基础上，听取公民对在具体场景下应用识别公民信息技术的意见，对信息识别技术的具体应用方案进行优化和修正。最后，还应根据不同应用场景，向上级主管部门和相关的行政管理机构进行备案和审批。在获得相关机构的批准后，行政机构才可以具体实施某一场景下信息的识别收集处理工作。在事中实际

进行个人信息的识别收集处理中，应严格遵循法律规定以及在备案中所列明的职责权限。在个人信息识别收集之前，应当对公民予以充分的知情告知，并根据不同具体场景的特点采取恰当的表达同意方式，不得侵犯公民的知情同意权和选择权。同时，行政机构应当采取必要的信息技术措施保护收集到的人脸识别信息。在完成相关信息识别处理后，需要及时删除收集到的个人识别信息或进行匿名化处理。对于行政机构工作人员在收集处理过程中的违法行为则依法追究其责任。

3.3. 坚持个人信息识别收集中的比例原则

比例原则是行政法领域的一项重要原则，包括适当性原则、必要性原则和狭义比例原则三个子原则。适当性原则，即行政部门采取的手段有助于行政目的的实现；必要性原则即行政部门在诸多可实现目的的手段中，选择对行政相对人侵害最小的一种；狭义比例原则，则要求行政机构采取的措施与其要达到的目的相称[27]。坚持个人信息收集中的比例原则，即避免以维护公共利益之名任意收集、处理公民的个人信息，追求社会公共利益与私人利益之间的平衡。

具体来说，第一应通过立法规制，明确界定行政机构基于公共利益追求，可以应用个人信息识别技术的场景、收集个人信息的范围限制、获得公民知情同意的方式，以及以列举加概括式的方式限定无须获得公民知情同意的特殊情形。通过完善立法，为行政机构收集处理人脸识别信息提供清晰的指引，避免行政权力无限扩张侵犯到公民的合法权益；第二，坚持基于公共利益使用个人信息识别技术时“法无授权不可为”的原则，在有可替代方式能够同样达到收集、处理目的时，就应该审慎评估个人信息识别收集技术的应用；第三，在对个人信息进行收集、处理的过程中，行政机构应当遵循“数据收集最小化”原则，减少对个人信息权益的侵犯。在收集方式、收集频率和收集数量上，与实现相应公共目的需求相适应，避免无序收集和肆意扩张。

参考文献

[1] 余成峰. 信息隐私权的宪法时刻规范基础与体系重构[J]. 中外法学, 2021, 33(1): 32-56.

[2] 刘苏雅, 柴嵘. 我国取得疫情防控重大决定性胜利[N]. 北京日报, 2023-02-24(010).

[3] 博登海默. 法理学[M]. 北京: 法律出版社, 2015: 79.

[4] 陈兵. 抗击新冠肺炎疫情中个人信息保护的法治慎思[J]. 社会科学辑刊, 2020(2): 23-32.

[5] 何勇. 泄露患者隐私, 湖南一区卫健局副局长被查处[EB/OL]. https://wap.peopleapp.com/article/5089342/4984606, 2020-01-30/2023-07-11.

[6] 孟涛. 公共卫生紧急状态法治的原理与建构——基于新冠肺炎疫情的研究[J]. 法学评论, 2020, 38(2): 135-147.

[7] 张炜达, 呼啸. 大数据时代下个人信息行政公益诉讼制度之建构[J]. 西北大学学报(哲学社会科学版), 2020, 50(4): 69-80.

[8] 敬力嘉. 大数据环境下侵犯公民个人信息罪法益的应然转向[J]. 法学评论, 2018, 36(2): 116-127.

[9] 何艳玲, 肖芸. 问责总领: 模糊性任务的完成与央地关系新内涵[J]. 政治学研究, 2021(3): 114-126+163-164.

[10] [英]恩迪科特. 法律中的模糊性[M]. 程朝阳, 译. 北京: 北京大学出版社, 2010: 41-73.

[11] [美]杰里·马肖. 贪婪、混沌和治理[M]. 宋功德, 译. 北京: 商务印书馆, 2009: 224-238.

[12] [英]米切尔·黑尧. 现代国家的政策过程[M]. 赵成根, 译. 北京: 中国青年出版社, 2004: 110-121.

[13] [美]詹姆斯·G.马奇, 马丁.舒尔茨, 周雪光. 规则的动态演变——成文组织规则的变化[M]. 童根兴, 译. 上海: 上海人民出版社, 2005: 22-41.

[14] 姜涛. 新罪之保护法益的证成规则——以侵犯公民个人信息罪的保护法益论证为例[J]. 中国刑事法杂志, 2021(3): 37-55.

[15] 类延村, 徐洁涵. 个人信息法律保护的权利基础与实践逻辑[J]. 图书馆建设, 2021(1): 84-92.

[16] 夏金莲. 大数据时代疫情防控中的信息披露与隐私保护[J]. 西昌学院学报(社会科学版), 2020, 32(3): 42-48+114.

[17] 徐勇. 基于中国场景的“积极政府” [J]. 党政研究, 2019(1): 5-10.

[18] 曾智洪, 游晨, 陈煜超. 积极型政府数字化危机治理: 动员策略与理论源流——以抗击新冠肺炎疫情为例[J]. 电子政务, 2021(3): 61-72.

[19] 赵西巨. 从知情同意原则的历史渊源和发展轨迹看其所保护之权利及其性质[J]. 南京医科大学学报(社会科学版), 2005(4): 304-308.

[20] 王士博, 王海霞. 区块链技术与个人数据保护规范的内源性冲突及调和路径——以欧盟 GDPR 为例[J]. 情报杂志, 2023, 42(2): 142-150+165.

[21] 高志宏. 大数据时代“知情-同意”机制的实践困境与制度优化[J]. 法学评论, 2023, 41(2): 117-126.

[22] 郭旨龙, 李文慧. 数字化时代知情同意原则的适用困境与破局思路[J]. 法治社会, 2021(1): 26-36.

[23] 韩旭至. 个人信息保护中告知同意的困境与出路——兼论《个人信息保护法(草案)》相关条款[J]. 经贸法律评论, 2021(1): 47-59.

[24] Wee, R. (2013) Dynamic Consent in the Digital Age of Biology. *Journal of Primary Health Care*, **5**, 259-263. https://doi.org/10.1071/HC13259

[25] 石佳友, 刘思齐. 人脸识别技术中的个人信息保护——兼论动态同意模式的建构[J]. 财经法学, 2021(2): 60-78.

[26] 田野. 大数据时代知情同意原则的困境与出路——以生物资料库的个人信息保护为例[J]. 法制与社会发展, 2018, 24(6): 111-136.

[27] 陈征. 论比例原则对立法权的约束及其界限[J]. 中国法学, 2020(3): 146-164.