情报工程 ISSN: 2095-915X
第1卷 第6期 62-66 2015 年 12 月
TECHNOLOGY INTELLIGENCE ENGINEERING
ISSN: 2095-915X Vol.1 No.6 62-66 Dec 2015

doi:10.3772/j.issn.2095-915x.2015.06.009

大数据时代的公权力监控与个人隐私保护

徐昊

（中国人民公安大学反恐怖学院 北京）

摘要：公权力监控与个人隐私保护是一个自从有了国家便存在的矛盾，只要国家还存在，这个矛盾就不会消失。整个人类社会就是在双方的不停博弈中不断前行。但是大数据时代的到来加剧了这一矛盾的冲突。公权力在大数据时代到来后，获取公民隐私的手段与程度都空前加强。这虽然对维护整个社会治安稳定做出了巨大的贡献，但是也严重的侵害了公民的个人隐私，引发了人们对个人权利的严重忧虑。两者间虽有本质矛盾，但又非不可调和。本文旨在探讨一种公权力监控的运用方式，使其既能满足我国维护社会长治久安的政治目的，又能使民众最大程度的保护期个人隐私并接受其对个人隐私的合理利用。

关键词：大数据，公权力，监控，个人隐私

Public Power Monitoring and Personal Privacy Protection During the Era of Big Data

Xu Hao

(School of Anti - terrorism, People's Public Security University of China, Beijing 100038)

Abstract: Public power monitoring and personal privacy protection is public problems since Countries are established. As long as there is country, this contradiction will not disappear. The whole human society is in constant game of both sides to go on. But the advent of the era of big data exacerbated this contradiction. After the arrival of the era of big data, public power increaseds the means and enhances the level of obtaining citizen's privacy. This situation is good for safeguard security of the whole society. But it is also a serious violation of civil privacy rights, causeing serious concerns for individual rights. Although there is a contradiction between public power monitoring and personal privacy protection, this article found a new way which could meet both side of the contradiction. The results of this way could both help the authorities to maintain the security of social and protect personal privacy.

Key words: Big data, public power, monitoring, personal privacy

作者简介：徐昊 (1991 －)，男，硕士研究生，研究方向：公安情报理论。

1 概述

大数据是继云计算、物联网之后 IT 产业又一次颠覆性的技术变革。云计算主要为数据资产提供了保管、访问的场所和渠道，而数据才是真正有价值的资产。企业内部的经营交易信息、物联网世界中的商品物流信息，互联网世界中的人与人交互信息、位置信息等，其数量将远远超越现有企业 IT 架构和基础设施的承载能力，实时性要求也将大大超越现有的计算能力。如何盘活这些数据资产，使其为国家治理、企业决策乃至个人生活服务，是大数据的核心议题，也是云计算内在的灵魂和必然的升级方向。

大数据时代网民和消费者的界限正在消弭，企业的疆界变得模糊，数据成为核心的资产，并将深刻影响公安情报的业务模式，甚至重构其文化和组织。因此，大数据对国家治理模式、对政策的决策、组织和业务流程、对个人生活方式都将产生巨大的影响。如果不能利用大数据更加贴近公民的生活现状、增加对大数据研判的深刻理解需求、进而高效分析信息并作出预判。

自 2005 年我国公安机关正式部署、实施情报主导警务战略以来，该战略展现了十分高效准确并且不可替代的作用。从 2005 年到 2015 年这十年间，情报主导警务战略不断完善，为维护整个社会的和谐稳定作出了巨大贡献。尤其是在 2013 年，大数据时代元年到来以后，情报主导警务警务这一模式的巨大潜力被进一步激发出来 [1]。

随着 2014 年 2 月 27 日，中央网络安全和信息化领导小组的成立。这个由中共中央总书记、国家主席、中央军委主席习近平亲自担任组长；李克强、刘云山任副组长的领导小组，将着眼国家安全和长远发展，统筹协调涉及经济、政治、文化、社会及军事等各个领域的网络安全和信息化重大问题，研究制定网络安全和信息化发展战略、宏观规划和重大政策，推动国家网络安全和信息化法治建设，不断增强安全保障能力。这也为情报主导警务战略的实施提供了新的契机。将大数据的理论、方法和技术应用于公安情报工作中，将使情报主导警务成为现实。因此在可见的未来，情报主导警务这一模式势必还会被进一步加强的与完善，大数据时代的到来也为其质变带来了有利催化的作用。

2 大数据时代使用智能研判的理论依据与发展现状

大数据时代到来后，公安部门大幅度提升信息化能力，进而带来了巨大社会稳定红利。但是随之而来的是对公民隐私权的侵犯不断加深。这种隐私权的侵犯有来自与大数据时代自身的属性，也有来自于公权力的侵犯。

在大数据自身属性方面，随着数字信息技术的不断发展，“网络匿名”有可能会变成“数学上不可能”的事。这个世界每年所创造的数据量在以指数形式增长，在 2011 年，这一数字则达到了 2.8ZB(1ZB =10244GB)，而且据知名信息行业咨询服务商 IDC 称，这一数字将在 2015 年翻一番。此外，这些数据中的 3/4 是由个体人在创造或移动数字文件时贡献的。举例来说，一个标准的美国上班族每年可以贡献 180 万 MB 的数据量，平均每天则有约 5000MB，这其中包括下载的电影、文档、电邮以及这些数据通过移动或非移动互联网传播时所产生的附加数据量。

尽管这其中的大部分数据都是不可见的，似乎也并不携带任何个人信息，但事实并非如此。现代数据科学已经发现几乎任何类型的数据都能用来识别创造它的人，就好比指纹一样。比如说你在网上下载的电影、你的手机发出的定位信息，甚至是你被监控摄像机所拍下来的步态都可以用

来识别你。实际上，数据越多，其中可以称得上隐私的就越少。普林斯顿大学的计算机科学家阿尔文德·纳拉亚南 (Arvind Narayanan) 称，只要有合理的商业动机来推动数据挖掘的进程，任何形式的隐私都是“算法上不可能”（algorithmically impossible）的。例如，Facebook 已经可以实现对个人信息收集的自动化与实时化，其首次公开募股时的财务档案显示，Facebook 上每位用户的图片和视频资料数据量约为 111MB，而 Facebook 的用户数如今已经超过了 10 亿 [1]。这在一些法律案件中，Facebook 所记录的数据也派上了用场，其中包括涉案人发过的文字信息、点过“赞”的东西以及所用过的电脑的 IP 地址等，这些资料加起来足有 800 页，这 800 页就又给每位用户增加了几 MB 的数据量。

与此同时，线上和线下的数据如今正在逐步融合，进而帮助营销人员更精准地进行广告投放，这也是众多“数字隐私”拥护者的烦心事。今年二月，Facebook 宣布与包括安客诚在内的多家数据代理商展开合作，通过整合各自的数据资源来构造现实世界与虚拟网络之间的联系。一个月后，安客诚的首席科学官在一次投资者会议上称他们的数据已经与全美 90% 的社会档案建立了链接。

这些数据往往被描述为“在某种程度上具有匿名性”，但是牵涉到的信息越多，这样的说法就越显站不住脚 [2]。就拿移动通信运营商来说，他们会记录用户的位置和手机号码，然后再将这些综合数据卖给商家。尽管位置数据的匿名化是可以实现的，但是来自 MIT 的伊夫·亚历山大 (Yves-Alexandre de Montjoye) 和塞萨尔·A·伊达尔戈 (César A. Hidalgo) 却发现只要通过同一手机的四个不同的位置数据点就可以精确定位其拥有者。不光是移动通信运营商，你所用的浏览器也会“出卖”你的个人信息，就连最近刚刚兴起的可穿戴设备（如 Google Glass）也被认为会引起隐私担忧。

另一方面，个别民警利用手中职权，在采集或使用过程中，故意调取，查看，下载分享公民的个人信息。甚至有些有意或无意将公民个人信息泄露，给当事人造成很大的精神与财产损失。2010 年 3 月 25 日发生的“胡亚事件”，便是其中的典型案例。这个案例中当事人胡亚因为真正的犯罪嫌疑人文某冒用其邻居胡亚的身份信息，有关部门在追究其刑事责任时没有到其户籍所在地核查其真实性，导致胡亚背上了“吸毒人员”，“违法犯罪人员”黑锅长达 8 年之久。

这一类行为不仅对整个公安工作，尤其是公安情报搜集，也就是情报主导警务模式的基础带来了巨大损害 [3]，（例如社区民警在开展人口管理与个人信息采集过程中，民众出于对个人隐私安全与对警方不信任等的种种原因填写错误虚假信息。）同时也使民众对我国政府的公信力造成巨大损坏。

与此同时，无论一个国家的民众怎么信任自己的政府，民众也不会将自己的核心隐私交于政府，或是任何公共团体中。隐私是个相对概念，具体取决于观众是谁。但是情报工作就是具有在侵犯个人或公共隐私的基础上，经过分析研判，得出对整个社会稳定的最优决策行动的属性。例如，对于恐怖分子来说，其轰炸某地标建筑物行动的方案对于其来说就是“隐私”，可若不将其行动的情报分析研判出来，就有可能造成不可估量的生命财产损失。每一个民众都想要追求绝对的安全与绝对的隐私保护，或者称之为绝对的自由。但这一目标在现阶段的人类社会是不可能实现的，民众必须在这两者中取舍。牺牲可承受的隐私侵犯来换取一个更为安全的生存环境是大多数理性人的抉择，也是情报主导警务模式的社会学理论存在依据。

我们不会为了保护个人的绝对隐私而让社会

沦为肆意犯罪的天堂，但与此同时，即便某些警方行动会有助于降低犯罪，也要予以制止。例如，如果警方无需任何手续就可以闯入任何人的家中，那么凶杀、强奸和抢劫分子也许会更容易受到震慑；如果允许政府在每个人的家中安装摄像头，犯罪率可能也会大幅下降。如果允许警方当全面监控民众的谈话内容，来获取所需要的打击犯罪的通信信息，大量的犯罪问题都可以得到相当程度的预防，并可以得到解决。

然而，若对上述假设问题说不，也就意味着民众心知肚明的允许更大概率的犯罪发生，还是你宁愿让自己面对更大的危险，因为追求绝对意义上的人身安全从来都不是我们压倒一切的唯一的社会重点。

这一矛盾可以简单的概括为人民日益增长的对人身安全需求与个人隐私保护欲望增强的矛盾。但是随着大数据时代的到来，给这一矛盾的调和与解决带来了新的思路。在大数据时代到来前，对于公民隐私数据的收集与分析，都是由人工来完成的，这就相当于将公民自己的隐私暴露在陌生人面前。当情报搜集与分析的主要完成主体是人，或者说大量的研判与甄别工作由人来完成的时候，这种隐私被侵犯感觉就会一直存在。但如果将甄别与分析的大部分工作交由电脑来完成，这种感觉就会大幅降低。因为电脑只是不带任何情感的将每个个体进行数字化与模块化的分析，从中发掘可能的犯罪人员，个人隐私并不会受到侵犯，并且可以加大对其访问权限的设置，从而大幅降低公民个人隐私泄露的可能性。

3 电脑研判带来的隐私保护优势与其他优势

大数据时代的到来为电脑研判的时代打下了坚实的基础。大数据时代的到来带给公安工作，尤其是情报主导警务模式的最大红利就是我们得到的数据属性变得更加多了。这些信息不再仅仅是公民的身份证号码，籍贯，户口所在地以及家庭核心关系，也不仅仅是个人的通话记录，地理位置信息。大数据时代的信息变得更加个性化与专业化。比如在医学领域上，各种贴身式的智能设备如智能手环，已经可以检测一个人的生理体征，并且通过记录分析的方式来得到一个人的具体健康状况。[4] 在可见的未来，各个学科之间的交互与碰撞所得到的二次数据，或者是初始数据与二次数据，二次数据之间的数据碰撞得到的多次数据，这些数据所代表的个人“指纹式”信息，将会是情报主导警务模式，也是情报研判的最重要数据来源与研判依据。在可见的未来，随着整个社会的信息化程度不断加深。任何一个生活在这个社会的犯罪分子，只要其使用通讯设备，或者是社交软件，甚至是去医院就医，他的“指纹式”信息就会遗留下来，公安部门就可以通过这些“指纹式”信息最快的锁定犯罪嫌疑人，极大的降低打击犯罪成本，同时大幅降低产生冤假错案的概率。

具体来说，在智能获取地理信息位置的情报主导警务模式初级时代，我们是很难仅从出入迪厅的地理轨迹信息来区别经常光顾迪厅的人员与吸贩毒人员。但大数据时代到来后，若辅助以个人生理体征指数，电脑就很容易区分出那些是吸贩毒人员，从而使警方的打击更加精确与高效。而这也仅仅是公安学与地理学和医学学科碰撞的冰山一角。

但是对于个人来说，医患之间的隐私是十分重要的隐私。也是我们宪法与法律保护的对象。同样，任何一种可以锁定我们每个人的隐私数据，或者是经过对比碰撞后得出的二次或多级数据都是每个公民的重要隐私 [5]。我们无法想象将一个艾滋病患者的健康状况公之于众后他所面临的巨

大的社会压力，也无法保障一个未婚先孕的妈妈的生活不会受到隐私被侵犯的正常生活。我们一方面需要加强保护保护公民隐私权的立法，加强公权力对公民隐私利用的监督，保证其只是用来打击犯罪而不是进行其他的用途。但另一方面我们也需要看到，即使在保证隐私权方面做得最好的美国，也会存在如斯诺登向卫报记者格伦·格林沃尔德曝光的国安局对其公民隐私肆意侵犯的情况[6]。这就需要我们从整整个研判主题，也就是公安情报分析的主要职责行使的形式作出改变。

如前文所述，大数据时代的到来已经为电脑研判警务活动提供了重要基础[7]。虽然现在计算机的计算以及储存能力还不能满足这一分析研判的需要。甚至公安系统内部，以及政府的各个部门之间还不能打破彼此间的信息壁垒，更不用提整合各企事业单位，民营企业的信息资源了。但我们必须意识到，这是解决人民对于安全与隐私双重需要的较为稳妥与高效的解决方案。

通过电脑研判并不是使其代替人工研判。而是通过电脑的强大的数据处理能力来解决一些触碰公民个人隐私的基础数据处理过程。因为无论是各种数据碰撞模式，都是需要人工来进行算法的确定与不断改进。虽然这一模式在开始的时候可能会产生一些误判的情况。但电脑研判的初始阶段也必定会辅助大量的人工研判，这也是这一模式的自我进化的必然经过。

大数据时代的到来已经从根本上改变了人们的生活方式。公安机关的工作运行模式也要势必与之相适应。不同学科数据之间的碰撞所产生的特定结论，必将使人群的属性更为细致的区分，这样所带来的数据筛选后的犯罪分子甄别也就会更加的准确与高效。这种由计算机完成的分析与筛选并不会被直接采用，而是会用人工进行核实，这在进一步确保降低冤假错案的同时，也会降低公民隐私被泄露的几率。

参考文献

[1] 奥斯特瓦德 , 皮尼厄 . 商业模式 新生代 [M]. 北京: 机械工业出版社 , 2014.

[2] Hubert2014. 大数据时代，我们还有隐私吗 [EB/OL][2013-5-15]. http://www.guokr.com/article/437013page=2.

[3] 彭知辉 . 大数据 : 让情报主导警务成为现实 [J]. 北京 : 情报杂志 , 2015(5):3-4.

[4] 吴汉华 . 大数据时代中如何进行医疗数据挖掘与利用 [J]. Silicon Valley.2014(5):12-13.

[5] 朱慧 . 网络用户的信息隐私边界及其敏感度等级研究 [J]. 广东工业大学学报 .2013(12):27-28.

[6] 冯登国 . 大数据安全与隐私保护 [J]. 计算机学报 .2014(1):249-249.

[7] 赵倩倩 . 大数据崛起与数据挖掘刍议 [J]. 电脑知识与技术 .2014(1):7832-7832.