基于电信运营商大数据的公共安全新策略

王 鑫
中移（成都）信息通信科技有限公司 四川 成都 610041

摘 要：大数据是21世纪第二个十年最热门的关键词之一，而公共安全作为国家安全重要的组成部分，也已经成为国内各级人民政府的共识。本文详细讲解了大数据在电信运营商网络系统中产生、搜集、分析等内容，并举例说明这些数据是如何为政府安全部门提供及时公共安全预警信息，并为我国公共安全管理和智慧城乡安全建设提供技术支撑。

关键词：大数据；公共安全；电信运营商；智慧城乡

1 大数据概述

现在的社会是一个高速发展的社会，科技发达，信息流通，人们之间的交流越来越密切，生活也越来越方便，大数据就是这个高科技时代的产物。

对于“大数据”（Big data）研究机构Gartner给出了这样的定义。“大数据”是需要新处理模式才能具有更强的决策力、洞察发现力和流程优化能力来适应海量、高增长率和多样化的信息资产。

2 电信运营商与大数据

根据艾媒咨询的统计，截止2023年底，全球大约有1250多家电信运营商，而全球移动用户总量超过84亿户。而在中国国内，中国移动的手机用户数超过9.9亿户，达到9.91亿户，另外一家电信运营商中国电信也分别有4.08亿户（中国联通2023未公布手机用户数量）。

如此大规模的用户数量，是与近些年来4G、5G电信标准的商用及承载于通信标准上的各类应用场景分不开的。伴随着智能手机的普及，基础网络承载的移动互联网各类业务近几年迅猛发展，使得移动用户数在2013年后又呈现一次井喷式发展。

有数据显示，截止2023年底，国内三大运营商在网的手机用户，实名制比例为100%，这是一个在数量上仅次于全国户籍身份系统的超级实名系统，而且这个系统与户籍身份系统最大的优势和区别在于，这是一个动态的、流动的信息数据库，并且作为手机用户，其流动性远大于暂时没有手机的人员。

如此海量的用户数，带来了海量的用户基础数据及行为数据，而在电信运营商内部，用户的数据又可大体分为以下几种类型：

（1）用户基础数据：登记在HSS或用户信息数据库中的标志及静态数据。

（2）用户通话数据：更新并存储在话单服务器中的通话记录。

（3）用户上网数据：更新并存储在数据业务采集服务器中的数据。

（4）用户位置数据：通过2G/3G location update 或者4G/5G的TA更新来获取的位置数据。

（5）用户话单数据：计费服务器中定义用户月、季度、年消费情况的数据。

（6）终端基础数据：通过运营商网络注册登记后，将会获得用户的手机终端型号等硬件基础信息。

当然除此以外，还有相当多的数据，如用户漫游数据，用户切换数据，用户行为习惯数据等，但因为和本论题的讨论的相关性不高，这里不再展开讨论。

由于这些数据往往会涉及到个人隐私方面的问题，其大部分时间仅仅是静静的沉淀在各大核心机房的服务器数据库内，并没有展开过多的分析应用。本文的观点就是积极的探讨下面这个论题，是否可以做一些尝试，把部分不会影响到单个用户隐私的一些数据进行采集、提取，再利用数据挖掘用户标签等技术进行分析，用于人民群众公共安全方面的尝试及应用，做到数据“取之于民，用之于民”，在情理和法理上，都应该属于值得去推广实施的情形。

3 公共安全和公共安全管理概述

公共安全，是指社会和公民个人从事和进行正常的生活、工作、学习、娱乐和交往所需要的稳定的外部环境和秩序。

公共安全管理，则是指国家行政机关为了维护社会的公共安全，保障公民的合法权益，以及社会各项活动的正常进行而做出的各种行政活动的总和。

公共安全包含以下几个方面的内容：

（1）信息安全：信息安全主要包括五方面的内容，即需保证信息的保密性、真实性、完整性、未授权拷贝和所寄生系统的安全性。这其中又按照对象分为个人信息安全、国家信息安全、企业与其他单位信息安全等。

（2）公共卫生安全。

（3）公共出行规律安全。

其余诸如避难者行为安全，人员疏散的场地安全，建筑安全，城市生命线安全，人员疏散等也属于公共安全的有机组成部分，这里不再展开定义和讨论。

4 电信运营商的大数据在公共安全预警系统的探索

由于电信运营商的各类数据，其更新的频率极高，数据量较为丰富，同时也有相当多的历史累计数据可供搜集和分析，因此无论是长期、短期还是紧急预警，都有其施展的空间和利用的价值。

如我们最熟悉的用户通话数据和用户基础数据，我们可以通过大数据分析电信运营商的所有用户异常数据，如用户实名制办理后开通很快就出现每日频繁大量的极短的通话记录（如少于15秒），可初步判断此号码较为繁忙，可能是商务人士，推销类人员，但也可能是电信诈骗犯罪分子，从而从长期预警的角度把号码对应的相关信息提供给公安机关以及金融机构进行联合的数据分析及防范，防止电信诈骗对人民群众造成财产损失。

另外如特殊节日，如在圣诞夜，跨年夜，春节，元宵节，各类展会，宗教集会等日子，群众可能会出现人群在某个时间某个路段（区域）特别集中的情况，通过该路段（区域）覆盖的电信运营商无线基站，无线WIFI，天网摄像头等网络设备，可实时获取用户位置数据信息变化情况，而此信息将会对突发情况的预警及城市管理职能提供有益的数据信息。

5 电信运营商大数据在公共安全管理预警系统中的应用案例

5.1 大数据与电信诈骗的预防的“电信防诈骗信息系统”

案例解析：近些年来，因为移动互联网及社交软件、移动支付和银行APP的普及，电信诈骗的数额越来越高，诈骗的方式和骗术也日趋多样化，曾经出现过清华大学教授被电信诈骗1780万元这样的极端案例出现。

但无论采用哪种途径进行诈骗，都绕不开电信运营商的网络。因为电信诈骗和面对面的骗术及现金诈骗不同，所有的操作都要诈骗者和受害者双方借助于运营商的网络进行。因此我们可以利用运营商大数据进行相关数据分析，再进行针对性防范和事后追踪等手段防范和打击这类诈骗的产生。

应对措施：电信诈骗，防范永远是第一位的，从大数据的角度来说，如何尽量使用技术手段分析、处理，挖掘此类电信运营商的各种业务数据，以实现用较少成本来规避此类事件发生的可能，这就能充分体现电信运营商大数据分析的益处。

我们可以从以下思路进行分析和处理：

（1）对电信诈骗高发的省份、城市，上线基于电信运营商大数据的“电信防诈骗信息系统”，该系统对手机/固话/网络电话这三种方式发起的通话记录数量，以日、周、月等周期模型进行统计，对其中通话次数（包括主被叫所有通话）如超过一个阈值（如日均100个）的业务号码重点进行监控。

（2）对于超过日阈值的业务号码，对其发起通话被叫号码分布区域（按照省进行划分），可能存在以下几种情况：

I、主叫通话拨打归属地（或漫游主叫拨打漫游地）所在省份的电话占比较多（如超过60%），外地省份号码较少的情况。

II、主叫通话拨打归属地（或漫游主叫拨打漫游地）所在省份的电话占比不多（低于20%），外地省份电话较多且分布省份较为分散的情况。

III、主叫通话拨打归属地（或漫游主叫拨打漫游地）所在省份的电话占比不多（低于20%），外地省份电话较多且分布省份较为集中的情况。

根据电信诈骗大多跨省进行的大数据分析，我们需要重点监控II和第III这情况，对于外地省份主叫电话较多的这两种情况，我们再对其被叫通话的所占比例进行统计和分析，大体会产生以下三种情况：

a、被叫通话几乎没有，全部是主叫呼出的，如设定阈值8%以内。

b、被叫通话相比较来说占一定的比例，如设定阈值（8%-20%），在这个比例内就认定为另一种类型。

c、被叫通话和主叫通话比较均衡，无明显偏好情况。如呼入电话占比在20-90%之间。

d、被叫通话占比100%。

根据主叫被叫通话的占比模型再一次进行筛选，因为电信诈骗通常是对一批同一地区的泄露个人隐私的号码进行逐一拨打，因此对III-a这种类型需要重点监控，II-a这种情况需要进行更大周期的通话监控策略中进行判断。

（3）根据筛选出的III-a类型，再对其整体主叫通话的接通率进行分析，

x、主叫通话接通率正常，大约60-90%。

y、主叫通话接通率较低，大约20-60%。

z、主叫通话接通率很低，大约0-20%。

那么接听率较低和接通率很低的这两种情况就需要进一步重点进行监控，结合前面的数据排查筛选得到III-a-y和III-a-z。

（4）把III-a-y和III-a-z这两类号码的用户进行位置数据匹配整合，找出其是否存在位置数据集中的情况，再根据号码实名制信息，排除如正规注册的公司申请用于广告推销的号码，剩下的以个人名义申请的号码，并且多个实名人员的手机号码定位在相同的位置，因电信诈骗多为团伙作案，则这有相同位置数据的一批手机号码的拥有者有相当大的电信诈骗嫌疑。电信运营商可把通过此系统挖掘的这类用户转发给公安网监做进一步排查处理。

5.2 大数据与突发群众聚集潜在威胁预警

案例解析：在国内的许多大中城市，特别是人口超过500万的特大型城市，在诸如圣诞平安夜，元旦跨年夜，元宵节，大型体育赛事，大型展览会，宗教集会的日子，通常会在一些标志性或特定场合随机出现市民密度远远超过街道及场馆承载能力的情形。

如此情况下，市民的密度甚至可以高达一平米4-6人，整个区域人员密度极高，且还在不断的移动，极易出现公共安全事件。国内的例子就有上海2014年12月31日跨年夜，外滩景区发生人员踩踏事件，造成36人死亡，49人受伤。2014年1月5日，宁夏固原市西吉县北大寺发生踩踏事故，造成14日死亡，10人受伤。

应对措施：利用电信运营商大数据中的用户位置数据（用户位置登记信息），制作“突发人流数据预警系统”统计特定区域的无线基站在平日的登记用户数，并形成按照单个无线基站基于时间变化的用户量的实时波形图，并对基站历史峰值登记用户数量进行记录。

“突发人流数据预警系统”按照基站的历史最大登记用户数据，针对某些特定位置基站进行数据阈值配置：

（1）对达到历史峰值登记用户数量50%的特定基站设置黄色预警标签，在预警系统平台上提醒系统管理员进行初步处理，并利用互联平台及时提醒政府应急管理机构及公安交警部门加以关注，可派遣部分人力前往相应基站覆盖区域进行指挥疏散。

（2）对登记人数持续增加并达到历史峰值登记用户数量80%的特定基站设置橙色预警标签，在预警系统平台上再一次加强提醒系统管理员，并利用互联平台及时提醒政府应急管理机构及公安交警部门加以重视，并加派人力前往相应基站覆盖区域进行指挥疏散。

（3）对登记人数继续增加并达到甚至超过历史峰值登记用户数量100%的特定基站设置红色预警标签，在预警平台上持续不断提醒系统管理员，并利用互联平台反复提醒政府应急管理机构及公安交警部门进入紧急预案，按照预案派遣足量人力前往相应基站覆盖区域进行指挥疏散。

最新案例：2019年的2月19日19:30分，正月十五元宵节，成都地标性建筑339电视塔将举行别开生面的一场电子烟花盛宴。此事是成都过年传统项目，很早就开始宣传，知晓的市民非常的多，也对这项活动异常期待。当天中午，就开始有摄影师，记者等相关人士开始占据“最佳观测点”。随着时间越来越接近19:30，成都339电视塔附近方圆3公里内聚集了大量人群，附近的道路几乎瘫痪。通过人群聚集区域内的手机注册用户数统计测算，四川移动得出的数据已经超过了30万人，再配合电信运营商天网监控等现场实时摄像头传来的数据，人流已经严重超过区域内街道的负荷。上报相关信息后，成都市应急厅管理局决定启动预案，对该区域群众采取限流入内的紧急措施，并安排成都市交管局和成都市公安局下辖相关分局紧急加派警力协助疏散区域群众，并联系相关单位提前结束电子烟花的活动，正如后面大家看到的结果，此次电子烟花活动只播放了一轮不到10分钟就提前结束了。

这样的突发情况，实际上在每个大型城市都有可能发生，而基于电信运营商的基于用户登记及话务量等数据，可以从宏观上对此类事件进行及时有效的识别并及时预警。我们通常理解的人数众多，这类表述很多时候只能代表人们的主观体会，而准确获取区域内市民聚集程度的具体变化趋势和实时数据，才能够有效的为城市公共安全提供有效帮助，通过建立起电信运营商的“突发人流数据预警系统”，能够利用电信运营商大数据及计算机软件系统的便利性，通过提前预测有大量人员聚集的情况并建模，对重点区域和路段的历史峰值数据进行提取，并将实时数据纳入监控系统，设置阈值并按照不同阈值的制定不同等级的应急预案，从而实现公共安全预警的新思路。

6 结论

基于电信运营商的大数据对于国家公共安全的很多方面都有相当程度的实用性。借助于运营商内部积累并持续生成的海量数据，我们可以在打击电信诈骗，预防群体集会突发事件等角度进行更加深入的研究及探讨。虽然这些角度包含的课题不一定可以给电信运营商带来直接的财务营收，但其带来的社会效益和公益角度的价值却是无法估量的。

参考文献

[1] [英]维克托著,盛杨燕;周涛译.《大数据时代》:浙江人民出版社,2013.

[2]吴越.包容视角下公共安全管理的问题分析与对策探讨[D].武汉科技大学,2013.

[3]程科.新时期公共安全管理的内涵和外延[J].管理学家,2014,(14).