全球数据安全观察

总第 99 期 2022 年第 27 期

(2022.07.25-2022.07.31)

大数据协同安全技术国家工程研究中心

NERCBDS
大数据协同安全技术
国家工程研究中心

目录

政策形势

1、国务院办公厅发布《关于同意建立数字经济发展部际联席会议制度的函》

7 月 25 日，国务院办公厅发布《关于同意建立数字经济发展部际联席会议制度的函》，同意建立由国家发展改革委牵头的数字经济发展部际联席会议制度，以加强统筹协调，不断做强做优做大我国数字经济。

联席会议由国家发展改革委、中央网信办、教育部、科技部、工业和信息化部、公安部、民政部、财政部、人力资源社会保障部、住房城乡建设部、交通运输部、农业农村部、商务部、国家卫生健康委、人民银行、国务院国资委、税务总局、市场监管总局、银保监会、证监会等 20 个部门组成，国家发展改革委为牵头单位。

http://www.gov.cn/zhengce/content/2022-07/25/content_5702717.htm

2、最高人民法院发布《最高人民法院关于为加快建设全国统一大市场提供司法服务和保障的意见》

7 月 25 日，《最高人民法院关于为加快建设全国统一大市场提供司法服务和保障的意见》发布。

明确指出支持建设统一的技术和数据市场。加强科技成果所有权、使用权、处置权、收益权司法保护，妥善处理因科技成果权属认定、权利转让、权利质押、价值认定和利益分配等产生的纠纷，依法支持科技创新成果市场化应用。依法保护数据权利人对数据控制、处理、收益等合法权益，以及数据要素市场主体以合法收集和自身生成数据为基础开发的数据产品的财产性权益，妥善审理因数据交易、数据市场不正当竞争等产生的各类案件，为培育数据驱动、跨界融合、共创共享、公平竞争的数据要素市场提供司法保障。加强数据产权属性、形态、权属、公共数据共享机制等法律问题研究，加快完善数据产权司法保护规则。

https://www.court.gov.cn/zixun-xiangqing-367241.html

3、《海南省政府数字化转型总体方案（2022—2025）》印发

7 月 25 日，海南省发布《海南省政府数字化转型总体方案》(2022—2025)。

方案在夯实数据资源基础中明确指出，加强数据安全管理。健全数据分级分类标准，结合数据应用场景，最小化授权用户的访问范围，强化安全访问控制。充分利用区块链、隐私计算等技术，强化数据使用监控，加强数据使用全链路审计，确保数据来源可溯，数据使用有序、有据、可控和安

全。

在强化大数据能力底座支撑中强调要强化安全保障体系，包括强化安全管理责任、提升网络安全防护能力、提升数据安全防护能力。

https://mp.weixin.qq.com/s/ivxn5aGkWplx9_J7kzxEQw

4、人大法工委：抓紧制定个人信息保护法配套制度

中共中央宣传部 28 日举行“中国这十年”系列主题新闻发布会，介绍新时代全面依法治国取得的历史性成就。全国人大常委会委员、法制工作委员会副主任许安标表示，2021 年 8 月，全国人大常委会审议通过了个人信息保护法，已经在去年 11 月 1 日开始实施。这部法律坚持立足国情与借鉴国际经验相结合，聚焦个人信息保护领域的突出问题和人民群众的重大关切，在已有立法基础上，进一步细化、完善个人信息保护应遵循的原则和个人信息处理规则，明确个人信息处理活动中的权利义务边界，健全个人信息保护工作机制，对违反个人信息保护的行为设置了严格的法律责任，切实保护公民个人信息。

许安标强调，个人信息保护法的实施，有不少条款需要制定配套规定，比如**公共场所图像采集管理、个人信息安全管理、个人信息出境安全评估等具体制度**，对于这样一些配

套制度，有关部门已经出台或者正在抓紧制定。在制定个人信息保护法的同时，全国人大常委会还审议通过了数据安全法。总的来看，个人信息保护涉及的领域很广泛，我们将在相关具体立法中进一步完善有关制度，织密织牢个人信息保护的法律制度。

https://mp.weixin.qq.com/s/Is7N-rV3CYTAdZfsbB9keA

5、美国众议院通过《勒索软件法案》

近日，美国众议院通过了《报告来自被选为监督和监控网络攻击和勒索软件的国家的攻击法案》(也称为《勒索软件法案》)。拟议的立法将通过强制报告与勒索软件和其他攻击有关的跨境投诉来修订 2006 年美国安全网络法案。

《勒索软件法》主要针对俄罗斯、中国、朝鲜和伊朗，在提到涉嫌勒索软件攻击者时，特别指出了这些国家。它针对那些被指控对美国实施勒索软件攻击的国家的个人、政府或其他组织。

https://mp.weixin.qq.com/s/co5U9QEXiLtM6R5QshkRiA

技术、产品与市场

1、全国首款“数据安全自评估”APP 重磅上线

7 月 31 日，在 ISC2022“护航数字山河·数据安全协同创新”峰会上，贵州大数据安全工程中心和大数据协同安全技术国家工程研究中心联合推出全国首款“数据安全自评估”App，向各行各业免费提供数据安全自评估服务，帮助提升数据安全能力水位。

为贯彻落实国家相关法律法规和标准规范，让企业能够“零成本”了解自身数据安全能力，鼓励大家共同提升数据安全水位。“数据安全自评估”APP 依据“数据安全能力成熟度模型”国家标准，以“免费”的形式向社会公众开放，企业可通过实名注册后，开启“免费”的数据安全自评估，依据企业提供真实的、有效的信息，APP 能够在评估结束后，通过图表形式，直观展示该企业当前的数据安全现状，并给出提升建议。

https://mp.weixin.qq.com/s/wDS8vIRdCkQUhDwmfjyrLA

2、《2022 年数据泄露成本报告》的十大关键发现

根据 Ponemon 和 IBM Security 近日联合发布的《2022 年数据泄露成本报告》，**2022 年全球数据泄露规模和平均成本**

均创下历史新高，数据泄露事件的平均成本高达435万美元。

《2022年数据泄露成本报告》基于2021年3月至2022年3月期间对全球550家组织所经历的真实数据泄露事件的深入分析。报告的关键发现如下：

（1）关键基础设施零信任策略滞后；

（2）支付赎金并非有效策略；

（3）云安全不成熟的代价高昂；

（4）人工智能和自动化安全技术可节约数百万美元的泄露成本；

（5）网络钓鱼成为代价最高的数据泄露原因；

（6）安全人才短缺导致数据泄露成本飙升；

（7）医疗行业数据泄露成本高企不下；

（8）过度信任关键基础设施组织；

（9）支付赎金得不偿失；

（10）混合云的数据泄露成本较低。

https://www.secrss.com/articles/45193

3、《隐私计算与公共数据开放白皮书》发布

《隐私计算与公共数据开放白皮书》建议，各地可以在开放数据的实践中引入隐私技术，以构建多主体协同、全周期覆盖的数据安全保护能力。

具体来看：一是，**对于高风险数据，可从开放原始数据转向“数据可用不可见”**。通过引入隐私计算技术，让数据利用方仅能获得数据利用结果，无法获得与推理原始数据，从而在释放数据价值的同时，降低数据泄露风险。

二是，**构建全周期的数据管控能力**。利用隐私计算“数据流向可追溯”、“数据用法可控可计量”的技术特性，在数据开放利用的全周期监测各主体行为，既实现对安全风险的早预警、早发现、早处置，也为责任追查与事后救济提供依据。

三是，**从集中式开放走向分布式开放**。利用隐私计算“原始数据不出库”的技术特性，数据开放平台可仅提供数据目录与元数据，不再汇集各部门各机构的原始数据，以降低数据泄露的风险。

https://www.secrss.com/articles/45197

4、北京加快推进数据要素市场化配置 全国首个数据资产登记中心揭牌

7 月 29 日，2022 全球数字经济大会数据要素峰会上，北京国际大数据交易所数据资产登记中心（简称“登记中心”）揭牌。作为数据进入流通环节的核心机构，登记中心是北京市构建数据要素核心基础设施、推进数据要素市场化流通的

又一重要布局和重大探索。

据介绍，登记中心将在市经济和信息化局指导下，由北京国际大数据交易所主导建设，将围绕三大任务目标展开：基于北京市数字经济规则体系，建立数据资产登记相关政策和制度体系，为数据资产的登记提供规则依据和流程规范；依托区块链等先进技术搭建数据资产登记平台，发布数据资产凭证和数字交易合约，实现数据资产唯一性确权；打通数据资产登记平台和数据资产交易平台，探索建设数据资产登记-评估-交易-增值的生态体系，推动数据资产的开发利用和价值挖掘。

https://mp.weixin.qq.com/s/usKTYXm4VMcHX3TFfdJnKA

5、政务数据分类分级难点

数据安全是以数据为中心的安全，在流动过程中保护数据的使用安全。建设数据安全的前提是清楚数据的分布、使用情况和安全风险。然后才能从风险应对角度出发实施恰当的保护，根据数据敏感级别不同，配置差异化的保护策略，对数据实施保护。数据资产识别和分类分级是数据使用管理和安全防护的基础，为数据尤其是重要数据制定分类分级制度并依规管理，是实现数据安全目标的重要工作。

数据分类面临的痛点问题：（1）如何选择分类维度的问

题；（2）单一分类维度下的类别划分问题。**数据分级面临的痛点问题：**（1）定性到定量的问题。针对信息资源的分级，需要根据信息内容确定，目前没有科学的方法和范式支撑构建信息内容的数学模型，因此很难准确定量地进行数据内容描述。（2）分级的级数问题。在政府部门进行政务信息资源分级时，需要找到一个合适的级数，使得在使用过程中达到效率和安全管控的平衡。过多的分级会给实际使用带来困难，太少的分级又会使得管控难以准确地约束数据。（3）分级的粒度问题。以什么样的力度进行分级才可以既达到分级防护的目的，同时不影响正常的业务，是一个还有待进一步研究明确的问题。（4）分级的有效落实问题。有些地方政府专门成立了大数据管理部门，来规范政府部门对信息资源的共享使用，也出台了相关的数据共享条例、数据安全保障条例等，但是还缺乏完整的流程和环节来完成从数据梳理、数据分类分级到数据存储保护、数据共享使用。

https://mp.weixin.qq.com/s/5b-M10ELexWPc3_wbyJTVQ

业界观点

1、邬贺铨：数字文明时代，数字安全基础性作用日益突出

数字经济成为全球新一轮科技革命和产业变革的重要引擎，将开启人类数字文明新时代，数字安全的基础性作用日益突出。

近年来，我国陆续出台了《数据安全法》、《个人信息保护法》、《国家网络空间安全战略》、《关键信息基础设施安全保护条例》，相关部门联合发布了《网络安全审查办法》、《云计算服务安全评估办法》、《汽车数据安全管理若干规定（试行）》、《区块链信息服务管理规定》等，为数字安全的发展指明方向。在政策引导下，安全产业进入快速成长期，有效助力数字经济的发展不断呈现出井喷之势。但站在数字化建设的统筹高度看，数字安全也面临新的挑战，一个新的安全时代即将到来。

对此中国工程院院士邬贺铨认为，数字安全不再是一个单纯的技术问题，是涉及业务、管理、流程、团队等各方面的系统工程。数字安全需要国际合作，但基础是需要建立我国自主可控的数字安全技术、产品和服务的完整体系。

https://mp.weixin.qq.com/s/mtt0APuRATtG9PZVSg5ywA

2、樊友山：筑牢数字安全屏障应做到三个“新”

数字经济在突破传统生产要素的流动限制，促进市场效率的同时，也带来了不容忽视的信息安全问题，这就要求我们必须筑牢数字安全屏障。应积极推动数字安全技术新发展，发挥市场主体新作用，完善新规则，助力构筑数字经济安全新长城。

当前，我国正进入数字化转型、智能化升级的关键时期。数字安全形势较过往发生了重大变化，防御理念、防御体系、防御技术都亟待变革。对此，樊友山提出网络安全企业助力数字安全建设的三个关键点。网络安全龙头企业要发挥自身技术、人才优势和技术创新主体作用，开展数字安全基础理论创新、重大问题研究和核心技术攻关，助力数字安全技术创新发展。广大网络安全企业要提高政治站位，牢固树立总体国家安全观，加强与政府部门、产业链上下游企业协同，共同维护国家网络空间主权、兼顾安全和发展。各网络安全企业作为护网主力，要加强对网络安全产业发展规律的认识，积极推动网信领域法律法规不断完善，积极参与网络空间国际标准规则制定，助力形成良性的数据安全治理体系。

https://mp.weixin.qq.com/s/1voIBU03uONUa4W_CJLLMA

3、周道许：强化金融数据安全治理 夯实金融行业发展基础

金融数据安全已不再是行业内部的自律性要求，而是全方位、多层次、立体化的数据安全建设体系。清华大学金融科技研究院金融安全研究中心主任周道许出席并指出，当前金融数据安全治理存在三方面突出问题。一是数字技术日新月异，金融数据成为网络攻击的首选目标。二是金融机构在个人信息保护与网络安全方面因自身管理不到位而受监管部门处罚的案例屡见不鲜。三是金融数据跨境流动日益频繁，带来越来越大的潜在安全隐患，而我国在跨境数据安全评估、认证及保护方面的法律法规细则还有待完善。

对金融机构在加强数据安全治理方面，周道许提出了五条建议。一是开展数据安全顶层设计，二是完善数据安全治理机制，三是加强数据应用生命周期中的安全管控，四是优化数据安全运营体系，五是加强金融科技安全人才培养及员工安全意识教育。

对国家与金融行业在加强数据安全治理方面，周道许提出了四点建议。一是加快配套标准规范建设，二是开展数据安全认证与针对数据安全的 IT 审计工作，三是加快数据安全产业生态建设，四是推动建立跨境监管国际合作机制，提高国际话语权。

https://new.qq.com/omn/20220729/20220729A0A1FE00.html

4、肖钢：要把维护金融数据安全作为数据治理的首要任务

7 月 29 日，2022 全球数字经济大会数据要素峰会主论坛在国家会议中心召开。会上，全国政协委员、中国证券监督管理委员会原主席肖钢提到，一些金融机构仍存在一些短板。主要表现在以下方面：一是数字化转型战略不清晰。二是数据质量有待进一步提高。三是基础技术支撑不够。四是数据管理能力有待增强。

在数字经济时代，竞争已从过去的企业之间的竞争、产业集群之间的竞争进入到数字生态建设的竞争。要**进一步规范金融机构与互联网平台以及科技公司的合作**，对主要服务金融机构与金融业务的科技企业（平台）加强市场准入管理，落实金融数据共治的责任与机制。要**进一步提高实体企业和个人参与金融数据治理的积极性**，增强参与主体信用，提高自我防范意识，维护消费者合法权益。要**进一步加强对金融数据利用与保护的监管**，细化监管规则，发展监管科技，及时识别和防范新型数字金融风险。要充分发挥行业自律组织作用，加强数据伦理建设，促进数据治理与公平竞争。

要**进一步完善金融数据治理技术标准**，优化数据分析处理系统、数据集市、数据仓库以及大数据存储与计算平台等数据基础设施与应用系统平台，借助隐私计算等技术，实现数据可用不可见，确保金融数据的授权使用、脱敏使用、机

器使用。要针对金融行业数据管理标准化需求，**研究制定金融数据管理能力成熟度评估模型**，提升科学治理水平。要**探索开展对金融机构智能风控体系和数字金融服务能力的评价体系建设**，加强与国际同行的交流借鉴与合作，推动金融数据治理体系创新发展。

https://www.bbtnews.com.cn/2022/0729/446061.shtml

5、韩开创：加强消费者权益保护和信息安全是发展金融科技的应有之义

加强消费者权益保护和信息安全是发展金融科技的应有之义。腾讯金融研究院副院长韩开创表示金融消费者保护对金融监管和金融市场的稳定意义重大，对于现有金融消费者保护体系的挑战已日趋显现，其主要表现在以下三个方面：一是消费者自身金融素养和科技素养亟待提升。二是消费者面临的风险控制更加复杂。三是消费者的隐私权更容易受到侵害。对此韩开创建议至少从以下五个方面发力，全面推动消费者权益保护机制的完善：一是**加强金融消费者自我保护教育**。二是**利用科技手段做好金融消费者保护**。三是**加强金融创新产品的监管**。四是**健全消费者数据隐私保护制度**。五是**加大对金融犯罪活动的打击力度**。

同时，金融行业在大规模采用新技术实现业务创新的同

时，也面临着诸多新的风险和挑战：一是金融科技较传统的金融电子化具有更强的穿透性，并进一步模糊网络边界。二是金融科技趋向更强的金融属性，使信息安全问题变得更为复杂。三是金融科技多学科和多领域的交叉性特点导致信息安全决策变得更加困难。对此，他提出以下建议：一是**加强全民信息安全意识**。二是**推广应用个人金融信息保护标准**。三是**保障金融信息基础设施安全**。四是**提升金融科技应用安全水平**。

https://new.qq.com/omn/20220729/20220729A0A1DS00.html

数据安全事件

1、意大利税务局疑遭勒索软件攻击，78GB 数据失窃

2022 年 7 月 26 日消息，据意大利安莎社周一报道，意大利当局正在调查税务机构 l’ Agenzia delle Entrate 遭遇的数据被盗事件，期间约 78 GB 数据被泄露。

周一早些时候，频繁活动、臭名昭著的勒索软件团伙 LockBit 3.0 在其网站上发布通告，称已经从意大利税务局窃取到“100 GB 数据，包括企业文件、扫描副本、财务报告及合同”，并附有 6 张据称是文件样本的截图。

税务局方面立即做出回应，称已经立即要求 SOGEI SPA 做出反馈和澄清”。这里的 SOGEI SPA 是一家 IT 上市企业，负责管理财务技术基础设施，并进行一切必要检查。

https://www.secrss.com/articles/45104

2、去中心化音乐平台 Audius 遭黑客攻击，超 600 万美元被窃取

2022 年 7 月 27 日报道，据悉，上周末去中心化音乐平台 Audius 遭受了黑客攻击，攻击者窃取了超过 1800 万个 AUDIO 代币，总价值约 600 万美元。AUDIO 价格受此事件影响在一小时内骤降 17%。

Audius 是一个托管在以太坊区块链上的去中心化流媒体平台，艺术家可以通过分享他们的音乐来获得 AUDIO 代币，而用户可以通过收听这些内容来赚取代币。

根据 Audius 周日发布的事后分析报告，事件中的黑客利用了合约初始化代码中的一个错误，该错误允许其重复调用初始化函数。随后，攻击者为脱手赃物，以损失其价值的 5/6 为代价，在 Uniswap 上以 107 万美元的价格交易了所有盗取的 AUDIO 代币，然后通过 Tornado Cash 混币服务隐藏了被盗资金的踪迹。

https://www.secrss.com/articles/45166

3、黑客在暗网公开 Rust 开发的的某窃取程序的源代码

2022 年 7 月 25 日称，黑客在暗网公开了用 Rust 开发的的某信息窃取恶意软件的源代码。该恶意软件开发者声称只用了六个小时就开发出来了，它非常隐蔽，VirusTotal 返回的检测率约为 22%。Cyble 将其命名为 Luca Stealer，执行时它会从 30 个基于 Chromium 的浏览器中窃取数据，主要针对密码管理器浏览器插件。Cyble 报告已经检测到至少 25 个在野利用的 Luca Stealer 样本，尚不清楚这种新的恶意软件是否会被大规模部署。虽然该恶意软件由跨平台语言 Rust 编写，但目前其只针对 Windows 系统。

https://www.bleepingcomputer.com/news/security/source-code-for-rust-based-info-stealer-released-on-hacker-forums/

4、广东首例！广州一公司未履行数据安全保护义务被警方处罚

2022 年 7 月 26 日，广州警方公布了广东省公安机关**首例适用《中华人民共和国数据安全法》的案件**：广州一公司未履行数据安全保护义务被警方处罚 5 万元。

广州警方检查发现，某公司开发的“驾培平台”存储了驾校培训学员的姓名、身份证号、手机号、个人照片等信息 1070 万余条，但该公司**没有建立数据安全管理制度和操作规程**，对于日常经营活动采集到的驾校学员个人信息**未采取去标识化和加密措施**，系统存在未授权访问漏洞等严重数据安全隐患。系统平台一旦被不法分子突破窃取，将导致大量驾校学员个人信息泄露，给广大人民群众个人利益造成重大影响。

https://www.gzdaily.cn/amucsite/pad/index.html?id=1892079#/detail/1892079?site4&columnID=0

5、对 2021 年大规模数据泄露，美国 T-Mobile 达成 5 亿美元和解

2022 年 7 月 26 日，据外媒报道，美国电信运营商 T-Mobile 已同意因去年针对其网络系统入侵造成的客户敏感信息泄露而遭到的集体诉讼达成和解。

根据拟议的和解条款，该公司将向受影响的客户及其律师支付 3.5 亿美元。据报道，受影响人数可能多达 7660 万，其中许多人是 T-Mobile 客户。

此外，根据和解协议，T-Mobile 将在“2022 年和 2023 年的数据安全和相关技术”上投入约 1.5 亿美元。据 T-Mobile 称，这些努力将包括通过 Mandiant、埃森哲和毕马威“设计战略并执行计划，以进一步改造我们的网络安全项目”，并为员工和合作伙伴开展近 90 万次培训课程。

https://mp.weixin.qq.com/s/TwIKBDLfUqeLTVRqHa1DMQ

6、OneTouchPoint 披露影响 30 多家医疗保健公司的数据泄露事件

2022 年 7 月 29 日，据外媒报道，邮件和打印服务供应商 OneTouchPoint 披露了影响 30 多家医疗保健提供商和健康保险公司的数据泄露事件。

OneTouchPoint 总部位于威斯康星州哈特兰，为医疗保

健行业的组织提供印刷、营销执行和供应链管理服务。该公司本周透露，它最近成为勒索软件攻击的受害者，勒索攻击导致存储在其系统上的个人身份信息 (PII) 遭到破坏。

该公司表示，确定受感染的系统包含其客户提供的 PII，包括姓名、地址、出生日期、服务日期、服务描述、诊断代码、健康评估信息以及会员 ID。在其网站上的数据泄露通知中，OneTouchPoint 列出了 34 家受到影响的医疗保险公司和医疗服务提供商，但数字似乎远不止于此。

https://www.securityweek.com/onetouchpoint-discloses-data-breach-impacting-over-30-healthcare-firms?&web_view=true

7、圣卢克卫生系统披露了影响数万名客户的供应商数据泄露

2022 年 7 月 28 日，据外媒报道，圣卢克卫生系统周三发布新闻稿称，因供应商的违规行为，数万名客户受到数据泄露的影响。

该医院表示，供应商 Kaye-Smith 的违规行为可能暴露了大量信息，包括患者姓名、被保险人姓名、地址、电话号码、身份证号码、出生日期、社会安全号码的最后五位数字、服务描述、账单金额、未结余额、付款到期日和帐户状态。圣卢克卫生系统确定了 31,573 名受违规影响的个人，系统中

所有医院的客户/患者都受到影响。圣卢克表示，“目前没有证据”表明所暴露的信息已被使用。

https://boisedev.com/news/2022/07/27/st-lukes-data-breach/?web_view=true

8、英国纽波特市政网络遭黑客入侵，员工信息发生泄露

近日，外媒称英国纽波特市内部网络疑似遭到黑客入侵，在职和离职的市政员工个人信息疑似发生泄露，但外部客户数据没有受到事件的影响，所有在线城市功能均可以正常运营。据调查显示，英国纽波特市在 2022 年 6 月 8 日到 2022 年 6 月 9 日网络中发现未经授权的攻击行为，攻击者获取了存储在该市文件服务器上的诸多文件。 这些文件包含用于某些在职和离职雇员及其配偶和家属的人力资源和福利目的的信息，包括姓名、地址、出生日期、社会安全号码、用于直接存款的财务帐号以及与团体健康保险等相关信息。

https://whatsupnewp.com/2022/07/city-of-newport-advising-past-current-employeesof-potential-data-loss/

9、540 万 Twitter 帐户数据在黑客论坛挂售

2022 年 7 月 24 日报道，名为 devil 的黑客称其利用漏洞

访问了 5485636 名 Twitter 用户的信息，并以至少 30000 美元的价格进行出售。用于收集数据的漏洞于 1 月 1 被披露并于 1 月 13 日修复，可被未经身份验证攻击者用来通过电话号码和邮件来获取任意用户的 Twitter ID。攻击者表示他们在 2021 年 12 月就开始利用漏洞收集数据，现在已有感兴趣的买家与他们进行接洽。目前，Twitter 尚未确认此次泄露事件，而卖家已删除该广告。

https://securityaffairs.co/wordpress/133593/data-breach/twitter-leaked-data.html

10、俄罗斯邮政客户的数据泄露到网络

2022 年 7 月 29 日报道，俄罗斯邮政客户的数据出现在互联网上。发布的样本包含 1000 万行，其中包含：跟踪号（货件的跟踪号）、发件人/收件人的全名（或公司名称）、收件人的电话号码、发件人/收件人的城市/邮政编码、重量/装运状态、出发日期/时间。

https://www.fontanka.ru/2022/07/29/71529368/