

你被“调”了什么？ 如何进行？

揭开职场上神秘“背调”的面纱

■ 劳动报记者 罗菁 制图 王陆杰

“背调”，对于职场人士来说，可谓是一个熟悉又陌生、欢喜又反感的词语。

不少人都曾经历过“背调”，可又不了解“背调”的内容；许多人都认为一旦接受“背调”，那离自己心仪的职位仅剩一步之遥，也有人质疑，认为“背调”是“背着劳动者偷偷摸摸调查”的行为，有侵犯隐私之嫌。

那么，“背调”到底会调查求职者哪些内容，谁在执行，是否会“一锤定音”，存在着哪些风险，又会不会侵犯职工权益……为此，本报记者经过对人力资源行业的多日采访，为你揭开神秘“背调”的面纱。

谁最容易“背调”？ 国企外企最多 金融科技涉及

“背调”，俗称入职前的背景调查。不过，业内人士告诉记者，并非所有职位都会“背调”，也不是每个行业都会进行“背调”。

从企业性质而言，国企可谓是“背调”大户。一家沪上知名的“背调”业务公司表示，通常而言，大型国企几乎所有的招聘职位，都会进行背景调查，这已经成为国企入职的必备程序之一。

其次，则是外企。虽然，外企没有国企职位要求范围这么广，但是对于“背调”的重视程度却是最高。换言之，如果在这一调查中出现哪怕与求职者所述一丝的不符合，外企很有可能就会将其拒之门外。

“通常来说，外企更看重求职者的诚信度。”一位负责“背调”的业内人士指出，曾有求职者简历中仅户籍一栏与“背调”结果不同，最终也被企业放弃。

另外，在外企和民企中，中高层职位接受“背调”的比例最高，而一线职员则极少，除非涉及核



心岗位。而这主要也是与岗位性质有关，此外“背调”的成本并不低，企业也要有所考虑。

就行业而言，金融业是“背调”的重中之重，包括投行、证券、基金、银行等，几乎无一例外会提出“背调”的要求；科技领域同样如此，主要是害怕出现同业竞争、知识产权、技术泄密等情况出现。

谁在进行“背调”？ 第三方是主流 兼自我调查

之所以要对求职者进行“背调”，关键在于用人成本较高，企业招揽人才风险也随之增大。

“看到过太多简历造假的事了。”一家大型人力资源公司招聘部门负责人告诉记者，虽然现在学历、学位“注水”的少了，但是在就业经历、历任职位、工作表现、获得成就等方面，仍有不少人“过度包装”。

用人不严，是企业大忌。为此，“背调”才会应运而生。早期，多为用人单位自查，由企业人事部门负责与“上家”沟通核实。但近年来，第三方专业公司成为主流，这些公司往往有各自的渠道，能获得大量求职者的信息，从中加以比对，从而验证出简历的真假。

“第三方服务之所以‘神通广大’，其实关键在于大数据。”业内人士告诉记者，“背调”公司并不是“私家侦探”，而是因为诸多开展这一业务的公司，其本身就从事人力资源行业，早期与诸多企业建立了合作关系，从而有庞大的数据库作为支撑。

“例如，沪上一家知名人力资源网站，就有‘背调’的业务，而借助其多年积攒的简历数据，通常很轻松就能找到相关资源。”该人士表示，除此之外，各行业的HR之间还有“圈子”和“交集”，这也

往往成为第三方专业服务公司的“突破口”。

如何对你“背调”？ 调查验证为主 须本人授权

而对于求职者来说，最关心的就是，“背调”究竟“调查”了哪些内容，又是如何进行的呢？

记者了解到，背景调查验证的信息一般包括候选人的身份户籍、不良记录、诉讼记录、学历学位、专业资格、商业利益冲突、工作经历、工作表现等，根据不同职位的要求，严苛度不一。

其中，学历学位、身份户籍、专业资格等最为容易查证，造假者也较少。水分比较大、不容易验证的，则是工作经历、工作表现、商业利益冲突等。而这，则是“背调”公司一展拳脚的时候。

“首先，‘背调’公司会对你的人事部门负责人、上级部门负责

人甚至公司总经理进行核实。”业内人士表示，其次，则会与求职者的同事、同级别负责人、下属进行沟通，“这种全范围的收集情况是必要的，以避免出现一面倒的说法。”

正是从这种“众说纷纭”中，“背调”公司可以从中核实一些关键性的要素，例如离职时间、离职原因、工作业绩、职位职务、业务能力等。

此外，根据特殊需求，“背调”公司还会与公安、民政、法院等政府职能部门进行沟通，合法获取其犯罪信息、诉讼信息、商业欺诈等。

不过，多位业内人士强调，所有这些业务的开展，都有个必需的准入条件，即调查前要获得被调查者的书面授权。

“换句话说，必须要获得求职者的许可。”一家大型人力资源公司招聘部门负责人告诉记者，如果求职者提出异议，就不得进行任何私下的“背调”，否则就会侵犯其个人隐私，“当然，如果求职者真的心仪这个职位，绝大多数都会愿意接受‘背调’。”

“背调”作用多大？ 一旦涉及造假 基本会出局

那么，在职场中，“背调”的作用究竟有多大呢？

对此，多家企业招聘负责人表示，通常而言，“背调”起到的是核实功能，是企业重要的参照内容，但也并不是以“背调”论英雄，还是要看求职者的个人能力和岗位符合度。有些虽有争议，但企业还是会慎重考虑，评估这个争议结果是否在他们能够承担的风险范围内，再决定是否按原计划录用人选。

但是，在部分中高层和核心岗位上，“背调”在关键时刻往往会一锤定音，尤其是一旦涉及“造假”、“注水”的行为出现，那么基本上就会“出局”。

网络安全人才数量缺口高达 70 万

新技术带来安全挑战 本质是“攻防对抗”

本报讯(劳动报记者 陈宁)当前，全球正进入以信息产业为主导的经济发展新时期，随着数字化、网络化、智能化深入各个行业领域，网络安全威胁和挑战愈加严峻，网络安全产业竞争也日趋激烈。在本届世界互联网大会上，来自产学研各界的专家聚焦5G、人工智能等新技术发展后带来的网络安全新态势，探讨如何应对网络安全新挑战，化解网络安全新威胁。

新技术带来 网络安全挑战

当前，5G、物联网、人工智能等技术的高速发展和普及，开启了第四次工业革命的浪潮。5G与人工智能等技术的融合，推动工业互联网、车联网、物联网发展的同时，也让网络空间变得更加复杂，并提出了更严峻的网络安全挑战。

比如基于人工智能的无人驾驶车辆被攻击，就可能车毁人亡；基于物联网的工业控制被攻击，就可能出现工厂停工，造成的损失和单纯的信息泄露不在一个量级。

从用户层面来看，例如物联网安全事件频发，对用户的隐私及财产安全造成重大损失。例如，在家中安装摄像头，原本只为了随时看到老人和孩子的活动情况，以便实时掌握家人的信息。但家庭智能摄像头里的隐私安全黑洞，却让原本科技提升生活品质的期盼，变成了一种威胁。

因此在应用新技术之前，一定要做安全评估，让新技术成为经济社会发展的助推器，而不是风险的引爆点。

网络安全本质 是攻防对抗

奇安信集团董事长齐向东

总结了当前网络安全形势的三大转变：一是网络攻击事件由小打小闹向国家大事转变；二是网络攻击技术由简单粗暴向复杂精细转变；三是网络攻击形式从通用型向APT攻击转变。

他提出了保护业务安全的三个构想：具备“免疫功能”，建立一个自适应的安全系统；做到“内外兼修”，拥有一个自主的安全系统；能够“自我进化”，成为一个自成长的安全系统。

“网络安全问题很多，目前最重要的挑战是APT。”360公司董事长兼CEO周鸿祎说，APT通常是有国家背景的黑客组织针对其他国家发起的网络攻击，用最先进的技术，通过长期持续的潜伏、渗透，达到窃取情报和破坏其他国家基础设施的目的。他透露，360公司多年来一共发现了近40起

其他国家针对中国基础设施的攻击。

“APT有点像传统战争中的隐身飞机，一般网络安全公司别说防范、对抗，看都看不到，而且蔓延潜伏的链条很长，可能会选择政府、军事、企业、个人等各种目标。”他说。

针对APT威胁，周鸿祎提出必须协同防御。以往网络安全公司在数据上没有协同，每个安全软件就像一个雷达，只能看到自己的一亩三分地，所有单位看到的都是碎片化信息，看不到全貌。“APT时代单点必败，必须攻防。”

人才数量缺口 高达 70 万

网络空间安全人才培养问题同样引起了各方关注。相关数据显示，当前网络空间安全人才数量缺口高达70万，预计到

2020年将超过140万。教育部网络空间安全专业教学指导委员会秘书长封化民指出，网络空间安全人才培养的数量远远满足不了社会需求，目前每年网络安全学历人才培养数量不足1.5万。

周鸿祎表示，网络安全的本质是人跟人的对抗。在这个领域里面，面临的对手都是很聪明的黑客，不是靠安装一套软件、硬件就能够简单地应对，所以人才基本上是一个网络安全最为重要的竞争要素。

同时，他还认为，要应对大规模的网络攻击，保障它的网络安全，那么未来网络安全行业一定是一个服务业，从这点来证明网络安全人才现在是这个行业最需要的。“现在我们正在和很多高校合作，多所高校都有网络安全学院，360今年也会推出相应的网络安全培训计划。”