

ملک می‌گوید، یکی دیگر از انواع این کلاهبرداری‌ها، دیپ فیک‌های تصویری است که مشابه همین الگوریتم است و برای یادگیری نیاز به نمونه تصویری دارد که اغلب در بستر وب موجود است. در این کلاهبرداری‌ها یک ماشین هوش مصنوعی که حرکات صورت و تصویر را شبیه‌سازی و پیامی را به قربانی منتقل می‌کند، ایجاد می‌شود. میزان این کلاهبرداری کمتر از دیپ فیک‌های صوتی و معمولاً در لایه‌های بالاتر رخ می‌دهد و برای اخاذی‌ها و سوءاستفاده‌ها انجام می‌شود. به گفته او یکی دیگر از این کلاهبرداری‌ها، فیشینگ است: «نمونه آشنای این نوع از کلاهبرداری لینک‌هایی است که برای افراد از طریق پیام کوتاه یا شبکه‌های اجتماعی ارسال می‌شود و با کلیک روی آن یک سوءاستفاده و کلاهبرداری مالی صورت می‌گیرد. در این‌روش هوش مصنوعی می‌تواند متن پیام، ایمیل یا پیام کوتاه حاوی لینک فیشینگ را شخصی‌سازی کند و درنهایت قربانی با یک پیام از یک فرد آشنا روبه‌رو می‌شود که همان ادبیات و کلمات آشنا را دارد و اطمینان قربانی جلب و روی لینک کلیک می‌کند. یادگیری هوش مصنوعی هم به‌واسطه پیام‌های ما در شبکه‌های اجتماعی در بسترهای مختلف است و با لحن و ادبیات کلمات ما آشنا می‌شود و می‌تواند پیام‌های ما را شبیه‌سازی کند.»

رئیس کارگروه ارتباط با صنعت کمیسیون هوش مصنوعی و علم‌داده نظام صنفی رایانه‌ای استان تهران تاکید می‌کند که در بسیاری از موارد در لایه‌ای دولتی و سطوح بالاتر جامعه، این فیشنگ‌ها برای سوءاستفاده اطلاعاتی صورت می‌گیرد و هرکاره برای جلب اطمینان افراد، یک ایمیل شخصی‌سازی‌شده برای افراد ارسال و او را وادار به کلیک روی یک لینک می‌کنند و درنهایت کلاهبرداری صورت می‌گیرد: «یکی دیگر از انواع کلاهبرداری با هوش مصنوعی مربوط به چت‌بات‌ها و ربات‌های پیش‌بینی‌کننده در بازارهای مالی است. هوش مصنوعی توان پیش‌بینی مدل‌های تکرارشونده و متغیرهایی که در بازار اثرگذارند را دارد، اما اغلب آنهایی که درحال‌حاضر در اختیار مردم است و روی آن تبلیغات انجام می‌شود، با هدف جمع‌آوری اطلاعات از کاربران و سوءاستفاده‌های مالی است و درعمل پیش‌بینی اتفاق نمی‌افتد؛ چون کاربر را درگیر روندی می‌کند که اطلاعات شخصی را در اختیار ربات قرار دهد

و در قبال آن، اطلاعاتی از وضعیت بازار دریافت کند، اما درعمل از اطلاعات مالی و شخصی افراد سوءاستفاده می‌شود. یکی دیگر از انواع این کلاهبرداری‌ها در شبکه‌های اجتماعی انجام می‌شود که طبق آن حساب‌های کاربری ساخته می‌شود که یک هوش مصنوعی آن اکانت را مدیریت می‌کند و طبق هدفی که برای آن ترسیم شده، می‌تواند جریان‌سازی، سوءاستفاده فکری، دریافت اطلاعات و انواع کلاهبرداری را انجام دهد. این حساب‌های کاربری غیرواقعی در دنیا و ایران در حال رشد است و نوعی دیگر از کلاهبرداری به کمک هوش مصنوعی است.»

ملک اضافه می‌کند که نوعی دیگر از این کلاهبرداری‌ها استفاده از ناآگاهی مردم درقبال استفاده از هوش مصنوعی است: «وقتی پدیده نوظهوری در جامعه رخ می‌دهد، افرادی به وجود می‌آیند که می‌خواهند از ناآگاهی مردم سوءاستفاده کنند؛ مثل دوره‌های هوش مصنوعی، آموزش هوش مصنوعی، پولدارشدن با هوش مصنوعی، پکیج هوش مصنوعی و موارد مشابه. یعنی هوش مصنوعی را به یک راهگشا که صرفاً با پرداخت پول و دریافت یک محتوا یا نرم‌افزار، اغلب مشکلات برطرف می‌شوند، تبدیل می‌کند اما بیشتر آنها سوءاستفاده و کلاهبرداری از قربانیان است.»

او به مردم توصیه می‌کند که چند نکته کلیدی را برای جلوگیری از قربانی شدن توسط هوش مصنوعی در نظر داشته باشند، به‌خصوص وقتی با کلاهبرداری با استفاده از دیپ‌ف یک و تماس صوتی نامعتبر روبه‌رو می‌شوند: «اگر با تماس‌های مربوط به درخواست کمک مالی از سوی افراد آشنا روبه‌رو شدید، صرفاً به یک صدا بسنده نکنید و اگر ممکن است تماس تصویری برقرار کنید یا آن تماس را قطع کنید و خودتان مستقیماً با فردی که تماس گرفته، تماس برقرار کنید تا بتوانیم تایید چندمرحله‌ای انجام دهیم. نکته دوم این است که اساساً کلاهبرداران از ترس و عجله قربانیان سوءاستفاده می‌کنند و آنها را در معرض تصمیم عجولانه قرار می‌دهند. در این شرایط باید خونسردی خود را حفظ کنیم تا تصمیمی عاقلانه بگیریم و درگیر هیجان و فشار آن تماس صوتی نشویم. تاجایی که ممکن است در یک بستر ناشناس، اطلاعات عمومی، از نشانی تا اطلاعات حساب بانکی خود را منتشر نکنیم. چون کلاهبرداران با در اختیار داشتن این اطلاعات، اعتماد قربانیان را جلب می‌کنند و می‌تواند حتی بدون اطلاع ما، کلاهبرداری کنند. حتی صدای خام ما می‌تواند یک خوراک برای یک ماشین هوش مصنوعی باشد که صدای ما را تقلید کند.» او تاکید می‌کند تا جای ممکن باید بدانیم در کدام لینک در حال پرداخت پول با وارد کردن اطلاعات هستیم. هرزمان دچار این کلاهبرداری‌ها شدیم بلافاصله به پلیس اطلاع دهیم و این تجربه را به اطرافیان انتقال دهیم: «به‌واسطه فیلترینگ گسترده در ایران، مردم مجبور به استفاده از فیلترشکن‌های مختلفی‌اند که همین ضریب امنیت را کاهش می‌دهد. وقتی آی‌پی ما، پایدار و مطمئن نیست و دائم در حال تغییر نباشد، راحت‌تر مورد سوءاستفاده قرار می‌گیریم.»

درخواست فوری انتقال پول یا ارسال کد تأییدشده است. در این‌روش، فرد تماس‌گیرنده خود را در موقعیتی اضطراری (مثلاً گرفتارشدن در بیمارستان به‌دلیل تصادف، نیاز سریع به پول و...) نشان می‌دهد تا قربانی فرصت بررسی با دقت بیشتر را نداشته باشد.» نوری در پاسخ به این پرسش که آیا می‌توان گفت کلاهبرداری با هوش مصنوعی در ایران رو به افزایش است؟ توضیح می‌دهد که ابزارهای تولید صدا، تصویر و متن به‌واسطه هوش مصنوعی، اکنون به‌راحتی در دسترس هستند و درمقابل، سطح آگاهی عمومی کاربران نسبت به این خطرها و تهدیدات بسیار کندتر رشد کرده است. به‌ویژه ترکیب این فناوری‌ها با روش‌های شناخته‌شده مهندسی اجتماعی، باعث‌شده تعداد و پیچیدگی حملات افزایش یابد.

شهروندان عادی چطور می‌توانند این موارد را تشخیص دهند یا پیشگیری کنند؟ نوری توصیه می‌کند هر نوع دریافت پیام متنی یا صوتی، همچنین تماس صوتی که درخواست فوری پول یا دریافت کد ورود به یک سرویس یا هر اطلاعات حساس دیگری دارد، حتی اگر صدا آشنا و متعلق به اعضای خانواده و افراد بسیار نزدیک هم باشد، باید مشکوک تلقی شود و تماس باید سریعاً قطع شود و از طریق تماس مستقیم (ترجیحاً تصویری) با شماره اصلی کسی که او را می‌شناسیم، صحت موضوع و درخواست را بررسی کنیم.

او از برخی اقدامات پیشگیرانه و مهم می‌گوید که می‌تواند امنیت ما در مقابل حملات را یک‌قدم بیشتر کند: فعال‌سازی احراز هویت دومرحله‌ای در همه حساب‌ها و پیام‌رسان‌ها و آموزش گسترده به‌خصوص به کودکان و افراد مسن درباره مفهوم «هویت جعلی دیجیتال» و خطر به اشتراک‌گذاری کدها و اطلاعات حساس: «در صورت وقوع هک یا سوءاستفاده به این روش‌ها، پس از خارج کردن دستگاه‌های هکر از حساب هک‌شده، حتماً از طرق مختلف (از طریق پست/ استوری در شبکه‌های اجتماعی یا روش‌های عمومی دیگر) مخاطبان را آگاه کنید. چراکه هریک از آن‌ها از طریق نصب بدافزاری که ممکن است از طرف شما برایشان ارسال شده باشد، می‌توانند حلقه بعدی این زنجیره کلاهبرداری باشند.»

➤ رشد نگران‌کننده کلاهبرداری با هوش مصنوعی در ایران

ارژنگ ملک، رئیس کارگروه ارتباط با صنعت کمیسیون هوش مصنوعی و علم‌داده نظام صنفی رایانه‌ای استان تهران به «هم‌میهن» می‌گوید، کلاهبرداری با هوش مصنوعی قطعاً در کشور در حال گسترش است؛ چون در همه دنیا با سرعتی بسیار زیاد در حال رشد است و در ایران هم سرعتی نگران‌کننده دارد. علت اصلی آن هم ناآگاهی مردم از این جنس کلاهبرداری‌ها و هوش مصنوعی است. علاوه بر این بسیاری از ابزارهایی که با کمک هوش مصنوعی کار می‌کند، ساده و رایگان در اختیار مردم قرار دارد؛ ابزارهایی مثل تقلید صدا تا دیپ فیک‌های تصویری و مدل‌های زبانی مختلف. خوراک این هوش مصنوعی‌ها هم برای یادگیری شامل صدا، تصویر خام و اطلاعات شخصی ماست که به‌صورت عمومی در بسترهای مختلف وجود دارد که کار را برای کلاهبرداران ساده‌تر می‌کند و این جنس کلاهبرداری هم روزبه‌روز در حال افزایش است.

ملک توضیح می‌دهد که هنوز آمار رسمی درباره رایج‌ترین انواع کلاهبرداری با هوش مصنوعی در ایران منتشر نشده، اما طبق گزارش‌های مردمی و پلیس، بیشترین کلاهبرداری‌ها در ایران با استفاده از هوش مصنوعی مربوط به دیپ فیک‌های صوتی است که از مردم کلاهبرداری مالی می‌کنند. مرحله بعد، فیشینگ‌های پیشرفته است. به‌واسطه ناآگاهی عمومی مردم نسبت به تکنولوژی، هنوز هم موارد زیادی از کلاهبرداری با لینک‌های جعلی کلاسیک توسط مردم دیده می‌شود، حالا تصور کنید که هوش مصنوعی هم به این حوزه وارد شود؛ در این شرایط حتماً ترخ آن افزایش پیدا می‌کند. مرحله بعد هم کلاهبرداری در قالب کمپین‌های مربوط به پیش‌بینی بازارهای مالی به کمک چت‌بات‌هاست.

رئیس کارگروه ارتباط باصنعت کمیسیون هوش مصنوعی و علم‌داده نظام صنفی رایانه‌ای استان تهران می‌گوید: «مهم‌ترین کلاهبرداری‌هایی که با هوش مصنوعی صورت می‌گیرد، دیپ فیک است که در بستر صوت و تصویر انجام می‌شود و قربانیان متعددی دارد. در ایران هم مهم‌ترین و بزرگترین کلاهبرداری‌هایی که با استفاده از هوش مصنوعی انجام می‌شود، در حوزه دیپ فیک‌های صوتی است. به این صورت که با صدای یکی از آشنایان، با فرد تماس گرفته و در سناریویی، یک شرایط بحرانی برای قربانی ترسیم می‌شود و غالباً در خواست وجه مالی می‌شود. هر ماشین هوش مصنوعی برای تقلید صدا نیاز به تعدادی نمونه صوتی دارد که به‌واسطه گسترش شبکه‌های اجتماعی، نمونه صدای افراد در دسترس است و به‌این ترتیب برای ماشین هوش مصنوعی میسر است که صدای افراد را تقلید کند. ازطرف دیگر، یک ماشین هوش مصنوعی دیگر که در زمینه تبدیل متن به صوت عمل می‌کند، وارد بازی می‌شود و هر متنی را که در اختیار آن قرار دهیم، با صدای تقلیدشده به قربانی کلاهبرداری ارائه می‌کند. این کار به‌راحتی می‌تواند اطمینان او را جلب کند و فرد، قربانی کلاهبرداری شود.»



ارژنگ ملک
 رئیس کارگروه ارتباط باصنعت کمیسیون هوش مصنوعی و علم داده «نصر» تهران:
کلاهبرداری با هوش مصنوعی در همه دنیا با سرعتی بسیار زیاد در حال رشد است و در ایران هم سرعتی نگران‌کننده دارد.

علت اصلی آن هم ناآگاهی مردم از این جنس کلاهبرداری‌ها و هوش مصنوعی است. علاوه بر این بسیاری از ابزارهایی که با کمک هوش مصنوعی کار می‌کند، ساده و رایگان در اختیار مردم قرار دارد؛

ابزارهایی مثل تقلید صدا تا دیپ فیک‌های تصویری و مدل‌های زبانی مختلف. خوراک این هوش مصنوعی‌ها و هوش مصنوعی است. علاوه بر این بسیاری از ابزارهایی که با کمک هوش مصنوعی کار می‌کند، ساده و رایگان در اختیار مردم قرار دارد؛

ابزارهایی مثل تقلید صدا تا دیپ فیک‌های تصویری و مدل‌های زبانی مختلف. خوراک این هوش مصنوعی‌ها هم برای یادگیری شامل صدا، تصویر خام و اطلاعات شخصی ماست که به‌صورت عمومی در بسترهای مختلف وجود دارد که کار را برای کلاهبرداران ساده‌تر می‌کند و این جنس کلاهبرداری هم روزبه‌روز در حال افزایش است

داده باشد، روبه‌رو نشده، باین‌حال باتوجه به اینکه این نوع از کلاهبرداری‌ها در جهان رخ می‌دهد، به‌زودی شاهد تشکیل پرونده دراین‌باره در ایران هم خواهیم بود: «در این نوع از کلاهبرداری‌ها از تکه‌هایی از صدا و ویدئوهای افراد استفاده می‌کنند و فیلم‌هایی را با هوش مصنوعی می‌سازند و برای خانواده‌ها می‌فرستند تا آنها را به پرداخت پول ترغیب کنند. برای مثال با هوش مصنوعی صدا را تغییر می‌دهند و می‌گویند، من را گروگان گرفته‌اند یا در بیمارستان هستم و در قالب یک تماس تلفنی به اشخاص نزدیک، درخواست پول می‌کنند. در کشورهای دیگر این موارد بسیار اتفاق افتاده و حتی به‌عنوان مدیرعامل شرکت، تماس صوتی با صدای تغییرداده شده به حسابدار شرکت گفته شده که پولی را به حسابی دیگر واریز کند. او از راه‌های پیشگیری از مواجهه با این کلاهبرداری‌ها گفت و توصیه کرد که شهروندان در چه اول به‌هیچ‌عنوان به تلفن‌های ناشناس پاسخ ندهند؛ چون ممکن است صدای آنها ضبط و شبیه‌سازی و به واسطه آن مشکلاتی ایجاد شود. او می‌گوید، دومین اقدام پیشگیرانه این است که مردم فیلمی از خودشان در شبکه‌های اجتماعی منتشر نکنند؛ چون ممکن است برخی کلاهبرداران به‌واسطه همین فیلم‌ها و به کمک فناوری دیپ فیک از آنها کلاهبرداری کنند. ازنگاه این وکیل دادگستری، سومین نکته‌ای که شهروندان باید دراین‌زمینه به یاد داشته باشند این است که اگر پیام متنی، صوتی یا ویدئویی از آشنایان خود دریافت کردند که در آن درخواست کمک مالی یا واریز پول مطرح شده بود، حتماً پیش از واریز، یکبار صحت این پیام را با خود فرد، بررسی کنند.

قانون جرائم رایانه‌ای در سال ۱۳۸۸ برای تعیین مصادیق استفاده مجرمانه از سامانه‌های رایانه‌ای و مخابراتی به تصویب مجلس شورای اسلامی رسید. انواع جرائم رایانه‌ای به سه دسته‌ی کلی تقسیم می‌شوند که شامل خرابکاری رایانه‌ای، کلاهبرداری رایانه‌ای و جاسوسی رایانه‌ای هستند. امروزه اصلی‌ترین حوزه مربوط به جرائم رایانه‌ای که پیگیری آن توسط وکیل جرائم سایبری انجام می‌شود، جرم هک و جرائم اقتصادی رایانه‌ای است که صرفنظر از ضررها و خسارت‌های اتفاقی که حاصل بی‌مبالاتی وارده به سامانه‌های رایانه‌ای است، به هفت دسته تقسیم می‌شوند: دسترسی غیرمجاز به دستگاه‌های پردازش داده، جرائم اقتصادی سنتنی به کمک پردازش داده‌ها (DP)، جرائم مربوط به رایانه علیه حقوق فردی، خصوصاً علیه حق حریم خصوصی شهروندان، کلاهبرداری از طریق دستکاری رایانه‌ای سیستم پردازش داده، جاسوسی رایانه‌ای و سرقت نرم‌افزار، خرابکاری رایانه‌ای و سرقت خدمات.

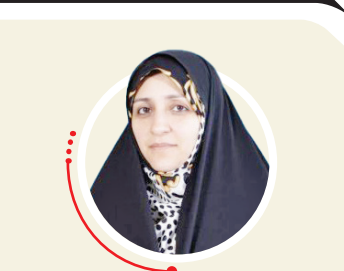
طباطبایی می‌گوید، موارد کلاهبرداری با استفاده از هوش مصنوعی نیز با استفاده از قانون جرائم رایانه بررسی می‌شود: «قانون مرتبط با این جرائم بسته به نوع نتیجه‌ای است که حاصل می‌شود؛ اگر نتیجه آن برداشت وجه از حساب کسی باشد، علاوه بر جعل رایانه‌ای، قانون مربوط به کلاهبرداری رایانه‌ای هم استفاده می‌شود. اگر برداشت وجه انجام نشود و صرفاً شخص به جعل اقدام کند، این اقدام جعل رایانه‌ای محسوب می‌شود. اگر فرد تصویر کسی را به‌صورت تقلبی بسازد و آن را منتشر کند، علاوه بر جعل رایانه‌ای، می‌تواند مشمول قانون مربوط به تصاویر مستهجن و مبتذل هم باشد. درنهایت نیازی به قانون جدیدی نیست و قانون جرائم رایانه‌ای آن را پوشش می‌دهد.»

➤ مراقب «دیپ فیک» صوتی باشید

در سال‌های اخیر نمونه‌های متنوعی از کلاهبرداری به روش مهندسی اجتماعی وجود داشت که طبق آن، کلاهبردار حساب تلگرام یا سایر پیام‌رسان‌های فرد قربانی را هک می‌کرد، سپس از طریق آن حساب، برای مخاطبان قربانی پیامی در راستای واریز وجه (مثل واریز پول بیمارستان به‌دلیل گرفتار شدن در شرایطی بحرانی) یا دریافت کد ورود به یک سیستم به‌پهانه‌های مختلف (مثل ارسال پیام برای گرفتن کد ورود دانش‌آموزان به یک پیام‌رسان از طرف حساب هک‌شده مدیر مدرسه به‌پهانه حضور و غیاب که اخیراً به‌صورت گسترده اتفاق افتاده بود) ارسال می‌کردند که باتوجه به ارسال پیام از طرف شخصی آشنا، اعتماد کاربر جلب می‌شد و روند کلاهبرداری از قربانی‌ها ادامه پیدا می‌کرد. این روش‌های مهندسی اجتماعی، حالا با ظهور ابزارهای هوش مصنوعی پیشرفته‌تر شده‌اند و توانایی جعل صدا، تولید متن‌های بسیار قابل‌باور و ساخت محتوای تصویری یا ویدئویی باورپذیر، سطح فریبکاری را به‌طور چشمگیری افزایش داده است.

میلاد نوری، برنامه‌نویس است و درباره انواع کلاهبرداری با هوش مصنوعی و مواردی که در ایران رخ‌داده به هم‌میهن توضیح می‌دهد. او می‌گوید، مهم‌ترین و فریبنده‌ترین انواع کلاهبرداری مبتنی بر هوش مصنوعی که امروز در ایران هم شاهد آن هستیم، عبارت است از دیپ‌فیک صوتی (Voice Deepfake) که در آن جعل صدای افراد آشنا برای جلب‌اعتماد و درخواست انتقال وجه، نصب اپلیکیشن مخرب و بدافزار به‌پهانه دریافت وام و مواردی دیگر یا گرفتن اطلاعات حساس مثل کد ورود به یک سیستم صورت می‌گیرد. او از موارد متعدد کلاهبرداری با جعل صدا در ماه‌های اخیر خبر می‌دهد و می‌گوید: «در ایران در ماه‌های اخیر موارد متعددی اتفاق افتاده که با صدای جعلی یکی از دوستان و آشنایان، با فرد قربانی تماس گرفته می‌شود و

خبرسازان



انتقاد از سهم کم زنان در اقتصاد

زهرای بهروزآذر، معاون رئیس جمهوری در امور زنان و خانواده با اشاره به شکاف‌های موجود در حوزه اقتصادی و سیاسی زنان گفته است که بیش از ۶۰ درصد ورودی دانشگاه‌ها را زنان تشکیل می‌دهند، اما تنها ۱۴ درصد از آنان در فعالیت‌های اقتصادی حضور دارند. همچنین از میان ۲۹۰ کرسی مجلس شورای اسلامی، تنها ۱۴ کرسی در اختیار زنان است. در انتخابات شوراها هم سهم زنان کمتر از ۱۰ درصد است. باید تلاش کنیم این نسبت افزایش یابد تا شهرها به فضاهایی مادرانه، خانواده‌محور و حامی زنان، سالمندان و کودکان تبدیل شوند. او با تاکید بر شنیدن صدای بی‌صدایان به‌عنوان یکی از رویکردهای اصلی دولت چهاردهم گفت: «هیچ ایرانی‌ای نباید احساس طرد یا نادیده‌شدن داشته باشد. در حوزه زنان، این مسئولیت سنگین‌تر است و ما موظفیم با برنامه‌ریزی دقیق، مانع حذف یابی‌توجهی به هر گروهی شویم. برای شنیدن صدای زنان، ابتدا باید همه‌مدیران ومسئولان توانمند شوند.»



هشدار درباره کاهش بودجه سلامت

سازمان جهانی بهداشت (WHO) هشدار داده که خدمات بهداشتی ضروری در برخی کشورهای کم‌درآمد و با درآمد متوسط، به‌شدت مختل شده است. به گزارش ایسنا، در بیانیه این سازمان آمده است، پیش‌بینی می‌شود کمک‌های بهداشتی خارجی تا پایان سال جاری میلادی (۲۰۲۵) در مقایسه با سال ۲۰۲۳، بین ۳۰ تا ۴۰ درصد کاهش یابد. سازمان جهانی بهداشت در راهنمای جدید خود برای کمک به دولت‌ها در واکنش به این بحران اعلام کرد که براساس داده‌های نظرسنجی جمع‌آوری‌شده در ماه مارس، کاهش شدید و ناگهانی بودجه، دسترسی به مراقبت‌های مادران، واکسیناسیون، نظارت بر بیماری‌ها و آمادگی اضطراری را در بعضی کشورها تا ۷۰ درصد کاهش می‌دهد. داده‌های ۱۰۸ کشور نشان داد که بیش از ۵۰ کشور نیز، از دست‌دادن شغل در میان کارکنان بهداشتی و وقفه در برنامه‌های آموزشی را گزارش کرده‌اند.



تداوم محدودیت‌ها در دانشگاه‌ها

رؤسای دانشگاه‌های تربیت مدرس و علامه طباطبایی از تداوم محدودیت‌ها در ارتباطات علمی دانشگاه‌ها با دیگر کشورها خبر دادند. به گزارش ایلنا، یوسف حجت، رئیس دانشگاه تربیت مدرس درباره ارتباط علمی دانشگاه‌ها با نهادهای علمی بین‌المللی گفت: «سال‌هاست که ارتباط‌های بین‌المللی ما به‌شدت کاهش یافته است. یکی از علل اصلی این موضوع، کمبود منابع مالی است. پیش‌تر اساتید ما به‌راحتی در کنفرانس‌های خارجی ازجمله در فرانسه شرکت می‌کردند اما اکنون با افزایش نرخ ارز، هزینه شرکت در یک کنفرانس خارجی برای دانشگاه بسیار بالا رفته است و این مسئله موجب‌شده بسیاری از اساتید نتوانند در این رویدادها حضور پیدا کنند.» او ادامه داد: «البته این ارتباطات به‌صفر نرسیده است؛ هنوز برخی اساتید با هزینه شخصی یا با کمک محدود دانشگاه در کلاس‌ها و کنفرانس‌های بین‌المللی شرکت می‌کنند، اما این موارد بسیار اندک است. بنابراین نخستین مانع اصلی ما، مسئله مالی است.» رئیس دانشگاه تربیت مدرس ادامه داد: «باتوجه به شرایط موجود، همکاری‌های علمی ما تنها به برخی کشورهای خاص محدود شده است و این موضوع نیز از کنترل ما خارج است. علاوه بر این مسائل، در داخل کشور نیز سختگیری‌های زیادی برای ارتباط با خارج از کشور وجود دارد. برای مثال گفته می‌شود اگر بخواهیم استادی خارجی را دعوت کنیم، باید چندماه پیش از آن اطلاع دهیم تا بررسی و تأیید شود. با برخی سازمان‌های بین‌المللی و کشورهای غیرمتخاصم نیز به ما اجازه همکاری نمی‌دهند.»