

کنٹرول کے سائے

پاکستان میں سنسرشپ اور بڑے پیمانے پر نگرانی

خلاصہ

AMNESTY
INTERNATIONAL



ایمنسٹی انٹرنیشنل 10 ملین افراد کی ایک تحریک ہے جو انسانیت کو متحرک کرتی ہے اور تبدیلی کے لیے مہم چلاتی ہے تاکہ ہم سب اپنے انسانی حقوق سے لطف اندوز ہو سکیں۔ ہمارا وژن ایک ایسی دنیا کا ہے جہاں اقتدار میں بیٹھے لوگ اپنے وعدے پورے کریں، بین الاقوامی قوانین کا احترام کریں اور جوابدہ ہوں۔ ہم کسی بھی حکومت، سیاسی نظریے، معاشی مفاد یا مذہب سے آزاد ہیں اور بنیادی طور پر ہماری رکنیت اور انفرادی عطیات سے مالی اعانت فراہم کی جاتی ہے۔ ہمیں یقین ہے کہ ہر جگہ لوگوں کے ساتھ یکجہتی اور ہمدردی سے کام کرنے سے ہمارے معاشرے بہتر ہو سکتے ہیں۔

©ایمنسٹی انٹرنیشنل 2025

← (CC)

جب تک کہ دوسری صورت میں نہ بتایا گیا ہو، اس دستاویز میں موجود مواد کریٹیو کامنز (Creative Commons) لائسنس (انتساب، غیر تجارتی، کوئی مشق نہیں، بین الاقوامی 4.0) کے تحت لائسنس یافتہ ہے۔
<https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode>
مزید معلومات کے لیے براہ کرم ہماری ویب سائٹ پر اجازت نامہ کا صفحہ ملاحظہ کریں: www.amnesty.org
اگر کسی مواد کا ماخذ ایمنسٹی انٹرنیشنل کے علاوہ کوئی اور کاپی رائٹ مالک ہو تو وہ مواد اس کریٹیو کامنز لائسنس کے تابع نہیں ہے۔

سرورق تصویر: ایک سلسلے میں کچھ کمرے ہیں جن میں لوگ اپنے ڈیجیٹل آلات استعمال کر رہے ہیں اور انہیں سیاہ بھوتوں کے ذریعے دیکھا جا رہا ہے جن کی آنکھیں سرخ ہیں اور وہ ان افراد کے اوپر منڈلا رہے ہیں تاکہ وہ دیکھ سکیں کہ وہ اپنے ڈیجیٹل آلات پر کیا کر رہے ہیں۔ تصویر کے اوپر درمیان میں ایک بڑی آنکھ لٹک رہی ہے جو دنیا کے نقشے کے اوپر ہے۔ اس آنکھ کی رگیں دنیا کے نقشے سے جڑی ہوئی ہیں جو دنیا بھر کے مختلف ممالک سے منسلک انٹرنیٹ ٹریفک کی نگرانی کر سکتی ہیں۔ © بشری سلیم

پہلی بار 2025 میں ایمنسٹی انٹرنیشنل لمیٹڈ
پیٹر بیننسن ہاؤس، 1 ایسٹن اسٹریٹ
لندن، UK WC1X 0DW سے شائع کیا
انڈیکس: ASA 33/0207/2025
اولین زبان: انگریزی

amnesty.org

AMNESTY
INTERNATIONAL 

خلاصہ

پاکستان کا غیر قانونی نگرانی اور آن لائن سنسرشپ میں ملوث ہونے کا ایک طویل اور تفصیلی ریکارڈ موجود ہے جو انسانی حقوق کے محافظوں، پسماندہ کمیونٹیز اور درحقیقت اس ملک کے ہر فرد کے انسانی حقوق کے لیے شدید خطرات کا باعث ہے۔ یہ سب کچھ ایسے ماحول میں ہو رہا ہے جہاں سیاسی فضا بڑھتے ہوئے جبر کا شکار ہے، جس میں آن لائن آزادی اظہار رائے کو جرم قرار دینے کے لیے ظالمانہ قوانین کا استعمال، احتجاج اور اجتماعات پر پابندیاں، من مانی گرفتاریاں، حراستیں اور جبری گمشدگیاں شامل ہیں۔ پاکستان کا قانونی نظام بڑے پیمانے پر نگرانی کے طریقوں کے خلاف تحفظ فراہم کرنے میں ناکام ہو رہا ہے کیونکہ ملکی قانون میں اہم حفاظتی اقدامات کی کمی ہے اور عملی طور پر قانون کو اکثر نظر انداز کیا جاتا ہے یا اس کا غلط استعمال ہوتا ہے۔ یہ رپورٹ ظاہر کرتی ہے کہ کس طرح پاکستانی حکام نے انسانی حقوق کے معیار کے مطابق اپنے رویے میں بہتری لانے کے بجائے مختلف عالمی کمپنیوں سے نئی اور جدید ترین نگرانی اور سنسرشپ کی ٹیکنالوجیز حاصل کر لی ہیں۔

اگرچہ اس طرز عمل کے نتیجے میں انسانی حقوق کی خلاف ورزیوں اور ان سے ہونے والے نقصان کی روک تھام کی بنیادی ذمہ داری پاکستان کی ہے اور وہ قانونی طور پر اسکا پابند بھی ہے تاہم اس کے حکام کئی سالوں سے ان سرگرمیوں کے لیے دوسرے ممالک کی نجی کمپنیوں سے خریدی گئی ٹیکنالوجی پر انحصار کرتے رہے ہیں۔ دوسرے بہت سے ممالک کی طرح ایسی خریداریوں میں اکثر شفافیت نہیں ہوتی جو بین الاقوامی انسانی حقوق کے معیارات کے خلاف ہے۔ اس غیر شفافیت کی وجہ سے برآمد کرنے والی کمپنیاں اپنی انسانی حقوق کی ذمہ داریوں کو پس پشت ڈال دیتی ہیں اور پاکستان کے لوگ آن لائن سنسرشپ اور نگرانی سے ناواقف رہتے ہیں۔

یہ رپورٹ ان عالمی نجی کمپنیوں کو بے نقاب کرتی ہے جو پاکستان کے آن لائن حقوق کے تحفظ میں خراب ریکارڈ کے باوجود غیر قانونی نگرانی اور سنسرشپ کے لیے ٹیکنالوجی فراہم کر چکی ہیں اور کچھ تو اب بھی کر رہی ہیں۔ یہ رپورٹ بتاتی ہے کہ کیسے ان کمپنیوں نے انسانی حقوق کی اپنی ذمہ داریوں کو کھلم کھلا نظر انداز کیا ہے اور یہ بھی کہ غیر ملکی ریاستوں نے ایسی ٹیکنالوجیز کی منتقلی کو مناسب طریقے سے کنٹرول کرنے میں اپنی ذمہ داری کو پورا نہیں کیا حالانکہ ان ممالک میں اس کے استعمال سے انسانی حقوق کو واضح خطرات لاحق ہونے کا احتمال تھا۔ اس رپورٹ میں پاکستان کے حکام اور ٹیلی کمیونیکیشن فراہم کرنے والوں کو بیچی جانے والی نگرانی اور سنسرشپ کی ٹیکنالوجیز کی تکنیکی تفصیلات شامل ہیں۔ یہ تکنیکی معلومات اس لیے دی گئی ہیں تاکہ یہ واضح ہو سکے کہ یہ ٹیکنالوجیز وقت کے ساتھ کیسے بہتر ہوئی ہیں اور یہ حکومتوں اس معاملے میں مطلب پاکستان کو بغیر کسی آزادانہ نگہبانی کے آبادی کی ایک بڑی تعداد کی نگرانی کرنے اور ان کی انٹرنیٹ تک رسائی یا کچھ ویب سائٹس کو کنٹرول کرنے کی اضافی صلاحیت کیسے دیتی ہیں۔ اس رپورٹ میں جن ٹیکنالوجیز کی بات کی گئی ہے وہ جدید ترین نگرانی اور سنسرشپ ٹیکنالوجیز ہیں جو ایک ہی وقت میں آبادی کے ایک بڑے حصے کی ذاتی معلومات تک رسائی ممکن بناتی ہیں جسے بڑے پیمانے پر نگرانی کہتے ہیں۔ اس کے علاوہ، ڈیپ پیکیٹ انسپیکشن جیسی ٹیکنالوجیز کی مدد سے حکام کے لیے ناپسندیدہ سمجھے جانے والے مواد یا VPNs کو بلاک کرنا آسان ہو جاتا ہے۔ اس رپورٹ کا مقصد پاکستان میں موجود نگرانی اور سنسرشپ کے ان طریقوں کا ایک قابل فہم جائزہ پیش کرنا ہے جنہیں اب تک خفیہ رکھا گیا ہے۔ اس رازداری کی وجہ سے معلومات تک عدم مساوات پیدا ہوتی ہے اور سول سوسائٹی کے لیے خود کو بڑے پیمانے پر نگرانی یا سنسرشپ سے بچانا مشکل ہو جاتا ہے۔

یہ رپورٹ ایمنسٹی انٹرنیشنل کی ایک سال تک جاری رہنے والی تحقیقات کا نتیجہ ہے جسے گریٹ فائر وال ایکسپورٹ کا نام دیا گیا۔ اس تحقیق میں انٹرسیک لیب¹، پیپر ٹریل میڈیا اور ان کے شراکت داروں ڈیا اسٹینڈرڈ، فالو دی منی²، دی گلوب اینڈ میل³، جسٹس فار میانمار⁴ اور دی ٹور پراجیکٹ⁵ بھی شامل تھے۔ پورٹ سے یہ انکشاف ہوا ہے کہ 2014 سے جرمن اور اماراتی کمپنیاں پاکستان کے ساتھ بڑے پیمانے پر ڈیجیٹل نگرانی کی ٹیکنالوجیز کی وسیع تجارت کر رہی ہیں جبکہ کینیڈین کمپنیاں 2016 سے اور امریکی کمپنیاں 2021 سے انٹرنیٹ سنسرشپ کی ٹیکنالوجی فراہم کر رہی ہیں۔ 2023 میں، چینی، امریکی اور فرانسیسی کمپنیوں نے پاکستان کی اپ گریڈ شدہ قومی فائر وال کے لیے ٹیکنالوجی فراہم کی۔

یہ ٹیکنالوجیز جن دو سب سے بڑے غلط استعمال کو ممکن بناتی ہیں وہ بڑے پیمانے پر نگرانی اور غیر قانونی انٹرنیٹ سنسرشپ ہیں۔ بڑے پیمانے پر نگرانی میں حساس ذاتی ڈیٹا جیسے فون کالز، ٹیکسٹ میسجز اور انٹرنیٹ سرگرمیوں کی بڑے پیمانے پر نگرانی، جمع آوری، ذخیرہ اندوزی اور تجزیہ شامل ہے اور یہ سب کچھ مجرمانہ سرگرمیوں کے معقول شبہ کے بغیر کیا جاتا ہے۔ پاکستان میں مسلح افواج اور آئی ایس آئی (ISI) لا فل انٹرسیٹ مینجمنٹ سسٹم (LIMS) کا استعمال کرتے ہوئے پاکستانی ٹیلی کمیونیکیشن فراہم کنندگان (جو ملک میں کام کرنے کے لیے LIMS کے ساتھ تعاون کرنے کے پابند ہیں) کے ذریعے آبادی کے ایک بڑے حصے کی ڈیجیٹل سرگرمیوں کی نگرانی کرتے ہیں۔ 2024 کے ایک عدالتی کیس میں یہ انکشاف ہوا کہ پاکستانی سکیورٹی ایجنسیاں یہ نگرانی بغیر کسی عدالتی وارنٹ کے کرتی ہیں۔ سبسکرپشن پر مبنی کمرشل ٹریڈ ڈیٹا بیسز کے ذریعے ایمنسٹی انٹرنیشنل نے یہ پتہ چلایا کہ ایک جرمن کمپنی یوٹیمیکو (Utimaco) اور ایک اماراتی کمپنی ڈیٹا فیوژن (Datafusion) نے زیادہ تر ٹیکنالوجی فراہم کی جو LIMS کو پاکستان میں کام کرنے کے قابل بناتی ہے۔ یوٹیمیکو کا LIMS حکام کو ٹیلی کمیونیکیشن فراہم کنندگان کے صارفین ڈیٹا کو چھاننے کی اجازت دیتا ہے جو بعد میں ڈیٹا فیوژن کے مانیٹرنگ سینٹر نیکسٹ جنریشن (McNG) کے ذریعے قابل رسائی ہوتا ہے۔ پاکستان میں بڑے پیمانے پر نگرانی کی ٹیکنالوجیز کے استعمال اور تعیناتی میں تکنیکی اور قانونی حفاظتی اقدامات کی کمی کی وجہ سے LIMS عملی طور پر غیر قانونی اور بلا تخصیص نگرانی کا ایک آلہ ہے جو حکومت کو کسی بھی وقت 40 لاکھ سے زیادہ لوگوں کی جاسوسی کرنے کی اجازت دیتا ہے۔

انٹرنیٹ سنسرشپ میں انٹرنیٹ پر مخصوص مواد کو بلاک کرنا، انٹرنیٹ کی رفتار کو کم یا کنٹرول کرنا یا اسے مکمل طور پر بند کرنا شامل ہے۔ پاکستان میں وکی پیڈیا، ٹک ٹاک اور ایکس جیسی ویب سائٹس اور سوشل میڈیا پلیٹ فارمز کو معمول کے مطابق بلاک کیا جاتا ہے اور انٹرنیٹ نیٹ ورک بندشیں عام ہیں۔ 9 مئی 2023 کے احتجاج اور فروری 2024 کے انتخابات کے دوران ملک گیر انٹرنیٹ بندشیں ریکارڈ کی گئیں جبکہ دیگر مواقع پر مقامی اور صوبائی سطح پر بھی بندشیں دیکھنے میں آئیں۔ آن لائن مواد کی شناخت اور اسے بلاک کرنے کے لیے پاکستان ٹیلی کمیونیکیشن اتھارٹی (پی ٹی اے) مقامی ٹیلی کمیونیکیشن فراہم کرنے والوں کے ذریعے ویب مانیٹرنگ سسٹم (WMS) کا استعمال کرتی ہے۔

موجودہ تحقیق اور سبسکرپشن پر مبنی کمرشل تجارتی ڈیٹا بیسز کی بنیاد پر، ایمنسٹی انٹرنیشنل کو پتہ چلا کہ ڈبلیو ایم ایس کا پہلا ورژن 2018 میں پاکستان میں ایک کینیڈین کمپنی سینڈ وائن (Sandvine) کی فراہم کردہ ٹیکنالوجی کا استعمال کرتے ہوئے نصب کیا گیا تھا۔ ایمنسٹی انٹرنیشنل کو 2017 کے تجارتی ڈیٹا میں ہی سینڈ وائن (Sandvine) کا نام ملنا شروع ہو گیا اور اس نے کم از کم تین پاکستانی کمپنیوں کو ساز و سامان بھیجا جن سب کا پاکستانی حکومت کے لیے کام کرنے کا ریکارڈ ہے۔ ان میں سے دو کے نام پہلے سامنے نہیں آئے تھے: SN Skies Pvt Ltd اور A Hamson Inc۔ اس کے علاوہ ایمنسٹی انٹرنیشنل کو ایک لیک کے ذریعے بھی یہ معلومات ملی ہیں جسے کنسورشیم کے ساتھ شیئر کیا گیا تھا اور ایمنسٹی انٹرنیشنل اسے جی ایچ ڈیٹا سیٹ (Geedge dataset) کا نام دیتی ہے۔ اس لیک سے یہ بھی انکشاف ہوا کہ پہلے والا ڈبلیو ایم ایس جسے ایمنسٹی انٹرنیشنل ڈبلیو ایم ایس 1.0 کہتی ہے بعد میں ایک چینی کمپنی جی ایچ نیٹ ورکس کی تیار کردہ نئی ٹیکنالوجی سے تبدیل

¹ انٹر سیک لیب، <https://interseclab.org/en/home-en/> (استفادہ بتاریخ 18 اگست 2025)

² پیپر ٹریل میڈیا <https://www.papertrailmedia.de/>، (استفادہ بتاریخ 18 اگست 2025) ڈیا اسٹینڈرڈ <https://www.derstandard.at/>، (استفادہ بتاریخ 18 اگست 2025)

³ فالو دی منی <https://www.ftm.eu/>، (استفادہ بتاریخ 18 اگست 2025)۔

⁴ دی گلوب اینڈ میل <https://www.theglobeandmail.com/>، (استفادہ بتاریخ 18 اگست 2025)

⁵ جسٹس فار میانمار <https://www.justiceformyanmar.org/>، (استفادہ بتاریخ 18 اگست 2025)

دی ٹور پراجیکٹ <https://www.torproject.org/>، (استفادہ بتاریخ 18 اگست 2025)

اور بہتر بنایا گیا۔ چائنا الیکٹرانکس کارپوریشن کی ایک چینی سرکاری کمپنی نے اپنی ذیلی کمپنی ELINC China Co Ltd کے ذریعے پاکستانی کمپنی ELC Solutions Pvt Ltd کو ہارڈ ویئر کے پرزے بھیجے۔ ایمنسٹی انٹرنیشنل کا خیال ہے کہ جی ایچ نیٹ ورکس کی فراہم کردہ ٹیکنالوجی چین کی "گریٹ فائر وال" کا ایک کمرشل ورژن ہے جو ریاست کا ایک جامع سنسرشپ آلہ ہے اور اسے چین میں تیار اور استعمال کیا گیا اور اب باہر بھی کیا جا رہا ہے پاکستان میں جی ایچ نیٹ ورکس کی جانب سے فراہم کردہ ڈبلیو ایم ایس کی تنصیب اور اسے فعال بنانے کا کام مختلف کمپنیوں کے سافٹ ویئر یا ہارڈ ویئر کے ذریعے ممکن ہوا جن میں امریکی کمپنی Niagara Networks کا ہارڈ ویئر فرانسیسی کمپنی Thales کا لائسنسنگ سافٹ ویئر اور چینی کمپنی New H3C Technologies کا سرور ہارڈ ویئر شامل ہے۔

یہ تحقیق مزید اس بات کو واضح کرتی ہے کہ کئی ممالک نگرانی کی ٹیکنالوجی اور اس کے لیے استعمال ہونے والے ہارڈ ویئر کی برآمدات کو کنٹرول کرنے اور ان میں شفافیت لانے میں مسلسل ناکام ہو رہے ہیں جو انسانی حقوق کے لیے سنگین خطرات پیدا کرتے ہیں۔ وہ کمپنیاں جو یہ برآمدات کر رہی ہیں انہیں انسانی حقوق کے حوالے سے مکمل تحقیق کرنی چاہیے تھی اور ایسے سسٹمز کی تنصیب اور دیکھ بھال کے انسانی حقوق پر پڑنے والے اثرات کا بغور جائزہ لینا چاہیے تھا۔ اسی طرح برآمد کرنے والے ممالک کے حکام کو بھی لائسنس یا آیا ان برآمدات کی اجازت دی جائے یا نہیں کا فیصلہ کرنے سے پہلے انسانی حقوق کے خطرات کا جائزہ لینا چاہیے تھا۔ رپورٹ یہ بھی ظاہر کرتی ہے کہ ایک بار جب کسی ٹیکنالوجی کو برآمد کر دیا جاتا ہے تو اسے ایک نئے سنسرشپ سسٹم کے لیے دوبارہ استعمال کیا جا سکتا ہے جیسا کہ سینڈوائن کے معاملے میں ہوا۔ مزید برآں یہ رپورٹ بتاتی ہے کہ کس طرح پاکستانی حکام نے ملکی قانون کی قانونی ضروریات کو نظر انداز کیا اور ٹیلی فون وائر ٹپنگ کے لیے متواتر وارنٹ حاصل کرنے میں ناکام رہے۔

ایمنسٹی انٹرنیشنل نے اس رپورٹ میں موجود تحقیقی نتائج پر متعلقہ سرکاری اداروں اور کمپنیوں کو تفصیلی سوالات بھیجے اور ان سے جوابات کی درخواست کی۔ تاہم اشاعت کے وقت تک زیادہ تر سرکاری اداروں اور کمپنیوں نے کوئی جواب نہیں دیا۔ جن انٹیس اداروں سے رابطہ کیا گیا تھا ان میں سے صرف نیا گرا نیٹ ورکس اور ایپ لاجک نیٹ ورکس نے ہماری درخواست کا جواب دیا۔ جرمن وفاقی دفتر برائے اقتصادی امور اور برآمدات کنٹرول (BAFA) اور کینیڈین ٹریڈ کنٹرولز بیورو نے ہمارے خط کی رسید کی تصدیق کی لیکن ہمارے سوالات کے جوابات نہیں دیے۔ اگرچہ ٹیٹا فیوژن سسٹمز اور یوٹیمیکو نے اکتوبر 2024 میں ایمنسٹی انٹرنیشنل کی طرف سے بھیجے گئے تحقیقی سوالات کا جواب دیا تھا اور ان کے جوابات اس رپورٹ میں شامل ہیں تاہم ان کمپنیوں نے رپورٹ کے نتائج کی تفصیل بتانے والے خطوط کا کوئی جواب نہیں دیا۔ آخر میں رپورٹ کی اشاعت کی آخری تاریخ سے پہلے جی ایچ نیٹ ورکس، ان باکس بزنس ٹیکنالوجیز پرائیویٹ لمیٹڈ، ایس این اسکائیز پرائیویٹ لمیٹڈ، اے ہیمسن انکارپوریشن، ای ایل سی سلوشنز، نیو ایچ تھری سی ٹیکنالوجیز، تھیلز ڈی آئی ایس، ای ایل آئی ایس سی چائنا کمپنی لمیٹڈ اور چائنا الیکٹرانکس کارپوریشن لمیٹڈ اور ان سے متعلقہ اداروں، پاکستان موبائل کمیونیکیشنز لمیٹڈ (جاز)، چائنا موبائل پاکستان لمیٹڈ (زونگ)، ٹیلی نار، یوفون، پاکستان ٹیلی کمیونیکیشن کمپنی لمیٹڈ، سائبر انٹرنیٹ سروسز پرائیویٹ لمیٹڈ، ہواے، ٹرانس ورلڈ ایسوسی ایٹس، پاکستان ٹیلی کمیونیکیشن اتھارٹی، وزارت انفارمیشن ٹیکنالوجی و ٹیلی کمیونیکیشنز/اگنائیٹ، انٹر سروسز انٹیلی جنس، متحدہ عرب امارات کا ایگزیکٹو آفس برائے کنٹرول و عدم پھیلاؤ، چینی وزارت تجارت، یو ایس ڈیپارٹمنٹ آف کامرس اور فرانسیسی وزارت اقتصادیات نے کوئی جواب نہیں دیا۔ متعلقہ اداروں سے ایمنسٹی انٹرنیشنل کے سوالات پر محدود جوابات نے اس رپورٹ کے ایک اہم موضوع کو مزید تقویت دی ہے: نگرانی اور سنسرشپ کی ٹیکنالوجیز کی تجارت اور ان کے استعمال کے حوالے سے شفافیت اور معلومات کی کمی۔


یہ رپورٹ پاکستان اور دنیا بھر میں ڈیجیٹل اور انسانی حقوق کے مزید انحطاط کو روکنے کے لیے انسانی حقوق پر مبنی نقطہ نظر کے ساتھ، فوری طور پر مضبوط حفاظتی اقدامات، زیادہ شفافیت اور مؤثر جوابدہی کے طریقہ کار کی ضرورت پر زور دیتی ہے۔

ایمنسٹی انٹرنیشنل انسانی حقوق کے
لیے ایک عالمی تحریک ہے۔ جب
ایک شخص کے ساتھ ناانصافی
ہوتی ہے تو یہ ہم سب کے لیے
اہمیت رکھتی ہے۔

مکالمے کا حصہ بنیں برائے رابطہ

contactus@amnesty.org 

www.facebook.com/amnesty 

+44 (0)20 7413 5500 

@Amnesty 

کنٹرول کے سائے

پاکستان میں سنسرشپ اور بڑے پیمانے پر نگرانی خلاصہ

اس رپورٹ میں اس بات کو دستاویزی شکل دی گئی ہے کہ کس طرح دنیا بھر کی مختلف نجی کمپنیوں نے پاکستان کو نگرانی اور سنسرشپ کی ٹیکنالوجیز فراہم کیں اور کچھ معاملات میں ابھی بھی کر رہی ہیں اس کے باوجود کہ آن لائن حقوق کے تحفظ کے حوالے سے پاکستان کا ریکارڈ پریشان کن ہے۔ نگرانی اور سنسرشپ کی ٹیکنالوجیز کی فروخت اور منتقلی میں شفافیت کی کمی نے ایک ایسی عالمی تجارت کو فروغ دیا ہے جس میں کینیڈا، چین، جرمنی، امریکہ اور متحدہ عرب امارات کی طرف سے پاکستان کو کی جانے والی برآمدات بھی شامل ہیں۔

اس رپورٹ میں بتایا گیا ہے کہ پاکستان میں بڑھتے ہوئے جبر کے سیاسی ماحول میں نگرانی اور سنسرشپ کے غلط استعمال کو روکنے کے لیے قانونی تحفظات کی کمی ہے۔ اس ماحول میں آن لائن آزادی اظہار رائے کو ظالمانہ قوانین کے ذریعے جرم قرار دیا جا رہا ہے، احتجاج اور اجتماعات پر پابندی لگائی جا رہی ہے، اور من مانی گرفتاریاں، حراستیں اور جبری گمشدگیاں ہو رہی ہیں۔ رپورٹ میں پاکستان میں قانونی اصلاحات کی تجاویز پیش کی گئی ہیں تاکہ نگرانی اور سنسرشپ کے غلط استعمال سے بچا جا سکے ساتھ ہی ان کمپنیوں کو بھی اقدامات اکی تجویز دی گئی ہے جو اپنی انسانی حقوق کی ذمہ داریاں پوری کرنے کے لئے اٹھانے ہوں گے۔