

## Предварительное правовое заключение УВКБ ООН об изъятии и обыске электронных устройств искателей убежища

### 1. Введение

Несколько европейских государств недавно приняли или в данный момент рассматривают возможность принятия законодательства, согласно которому органам государственной власти разрешается производить изъятие и обыск персональных электронных устройств, таких как мобильные телефоны и планшеты, в целях проверки и подтверждения личности искателя убежища, а также для оценки ходатайства о предоставлении убежища по существу, в том числе на предмет потенциальных рисков для безопасности и возможных оснований для исключения из сферы международной защиты.

УВКБ ООН признает законные интересы государств в стремлении установить личность лиц, находящихся на их территории, в том числе что касается тех индивидов, которые потенциально могли совершить деяния, подпадающие под положения об исключении из сферы международной защиты, или могут представлять угрозу для национальной безопасности, а также заинтересованность государств в обеспечении принятия решений в отношении убежища на основании всесторонней и максимально точной имеющейся информации.

Кроме того, в соответствии с устоявшимися и широко применяющимися правовыми принципами и практикой, искатели убежища и лица, принимающие решения о предоставлении убежища, несут совместную обязанность по установлению и оценке всех значимых фактов, а также по разъяснению неполных или противоречивых утверждений, касающихся существенных элементов ходатайства.<sup>1</sup>

Таким образом, УВКБ ООН признает, что могут иметь место ситуации, в которых такие меры как изъятие и обыск персональных электронных устройств искателей убежища могут быть оправданы для достижения этих правомерных целей. Однако для этого должны быть соблюдены определенные условия. Учитывая потенциальные последствия таких жестких мер, не следует в индивидуальных случаях допускать ограничения или отказа в правовых гарантиях, обеспечивающих защиту искателям убежища от незаконного изъятия или обыска персональных электронных устройств. Такие меры также не должны стать обычной практикой в процедуре предоставления убежища. Применять их следует только тогда, когда это необходимо для рассмотрения ходатайства.

В данном документе излагаются предварительные правовые комментарии и ключевые принципы, которые должны использоваться при формулировании,

---

<sup>1</sup> УВКБ ООН, *Руководство по процедурам и критериям определения статуса беженца согласно Конвенции 1951 года и Протокола 1967 года о статусе беженцев*, декабрь 2011 г., HCR/1P/4/ENG/REV. 3, п. 196, <http://www.refworld.org/docid/4f33c8d92.html>.

принятии и применении законодательства и практики изъятия и обыска электронных устройств искателей убежища.

## **2. Значимость и использование данных, полученных с электронных устройств**

Электронные данные, сохраненные на мобильных устройствах, зачастую содержат различные сведения личного и конфиденциального характера (например, личное общение, финансовые записи, история поисковых запросов браузера, GPS-локация, социальные сети и т.п.). Хотя некоторые из этих данных могут иметь непосредственное значение при рассмотрении ходатайства об убежище, многие не будут представлять интереса или даже будут подлежать особой защите, предусмотренной законодательством большинства государств, например, информация, на которую распространяется обязанность сохранения адвокатской тайны, а также медицинская информация. УВКБ ООН считает, что легкость доступа к электронным данным не оправдывает нецелевого, бессистемного или спекулятивного поиска информации.

Управление Верховного Комиссара также хотело бы подчеркнуть, что доказательная ценность электронных данных должна рассматриваться с большой осторожностью. Искатели убежища зачастую не используют в социальных сетях свои настоящие имена, в том числе с целью избежать наблюдения и возможного преследования либо потенциального вреда, который может быть причинен их близким в стране происхождения. Кроме того, в некоторых случаях надежность или точность цифровых и электронных доказательств может быть низкой, либо их легко можно изменить. Наконец, довольно распространенный характер имеют ситуации, когда мобильные устройства передаются другим людям или используются другими людьми, в том числе контрабандистами или торговцами людьми.

Эти факторы следует должным образом учитывать, проверяя информацию или иным образом оценивая достоверность ходатайства искателя убежища на основании информации, изъятая из электронных устройств. Более того, следует уделить должное внимание обеспечению доступа искателя убежища и/или его законного представителя к любым доказательствам, которые будут использоваться для принятия решения по ходатайству о предоставлении убежища.

## **3. Изъятие и обыск электронных устройств**

Важными аспектами в вопросе изъятия и обыска электронных устройств являются: право искателя убежища на уважение человеческого достоинства;<sup>2</sup> право на неприкосновенность личной и семейной жизни;<sup>3</sup> право на защиту персональных данных;<sup>4</sup> а также право владеть, использовать и распоряжаться своей законно

---

<sup>2</sup> См., к примеру, *Всеобщая декларация прав человека*, 10 декабря 1948 г., 217 А (III) (UDHR), Статья 1, <http://www.refworld.org/docid/3ae6b3712c.html>, *Международный пакт о гражданских и политических правах* (16 декабря 1966 г.) 999 UNTS 171 (ICCPR), Статья 10, <http://www.refworld.org/docid/3ae6b3aa0.html> и *Хартия Европейского Союза по правам человека*, 26 октября 2012 г., 2012/C 326/02 (Хартия ЕС по правам человека), Статья 1, <http://www.refworld.org/docid/3ae6b3b70.html>.

<sup>3</sup> См., к примеру, Статья 17, *Международный пакт о гражданских и политических правах и Европейская конвенция по защите прав человека и основоположных свобод, с изменениями, внесенными Протоколами № 11 и 14*, 04 ноября 1950 г., ETS 5, Статья 8, <http://www.refworld.org/docid/3ae6b3b04.html>.

<sup>4</sup> См., к примеру, Статья 12, *Всеобщая декларация прав человека*, Статья 17, *Международный пакт о политических и гражданских правах человека*, и Статья 8, *Хартия ЕС по правам*

приобретенной собственностью.<sup>5</sup>

Согласно этим правовым стандартам и практикам изъятие или обыск должны проводиться с *правомерной целью*, предусмотренной законом, и быть *необходимыми* и *соразмерными* для достижения такой конкретной цели, в то же время должно быть обеспечено наличие и соблюдение на практике соответствующих процедурных гарантий.

Управление Верховного Комиссара считает, что для того, чтобы изъятие и обыск электронных устройств были правомерными, должны применяться следующие принципы и гарантии:

a. Изъятие и обыск должны проводиться на основании свободного и информированного согласия соответствующего человека. Чтобы согласие было информированным, человек должен своевременно получить достаточную информацию относительно процедуры и ее цели и иметь доступ к консультациям, чтобы правильно понимать свои права, а также потенциальные последствия предоставления согласия или отказа от него.

b. Изъятие и обыск без согласия человека могут быть оправданы, только если они служат достижению правомерной цели, предусмотренной законом, проводятся компетентным органом и основаны на решении, принятом в ходе оценки, проведенной на индивидуальной основе (с учетом особенностей дела), в соответствии с применимыми правовыми гарантиями. Особую важность имеет оценка необходимости изъятия и обыска, а также влияния таких мер на соответствующего заявителя.

c. Изъятие и обыск могут проводиться только компетентным органом в соответствии с законодательно установленными полномочиями и гарантиями.

d. Если для достижения упомянутой цели (к примеру, для проверки и подтверждения личности человека) имеются менее интрузивные меры или методы, следует прибегнуть к их использованию.

e. Органы власти должны оставлять и хранить только те данные, которые *значимы и существенны* для цели изъятия, и только если они необходимы для выполнения этой цели (к примеру, для оценки ходатайства о предоставлении убежища, потенциальных оснований для исключения из сферы международной защиты или угрозы для национальной безопасности). Избыточные данные следует не сохранять, а своевременно возвращать или уничтожать, при условии, что это не нарушает каких-либо других прав соответствующего заявителя.

f. Изъятые данные следует хранить безопасным способом, а их дальнейшее использование ограничивается установленной целью, необходимой для данного дела. Кроме того, доступ к таким данным может иметь лишь уполномоченный персонал.

g. Изъятие имущества должно быть ограничено по времени, а изъятое имущество должно возвращаться владельцу после достижения указанной цели. Если необходимую цель можно достичь, скопировав соответствующие данные вместо изъятия самого устройства, необходимо прибегнуть к этому способу.

---

человека.

<sup>5</sup> Там же.

h. Действия, совершенные соответствующими органами власти и сотрудниками, которые представляют такие органы, никоим образом не должны приводить к изменению, замене или удалению данных, на которых впоследствии можно будет основываться в процедуре предоставления убежища.

i. В ситуации, когда представитель соответствующих органов считает необходимым получение доступа к оригинальным данным, такой человек должен иметь на это полномочия, обладать соответствующими специализированными знаниями и готовым предоставить доказательства с объяснением значимости и последствий своих действий.

j. Необходимо создать и сохранить контрольные пометки для проверки или иные записи всех процессов, которые применяются к цифровым доказательствам. Независимая третья сторона должна иметь возможность ознакомиться с такими процессами и прийти к такому же выводу.

k. Искатели убежища, устройства которых были изъяты и подвергнуты обыску, должны иметь доступ к эффективному средству правовой защиты для обжалования законности изъятия или обыска, а также для обеспечения возврата любых изъятых устройств.

**УВКБ ООН**

**04 августа 2017 г.**